

Scan Results

06/30/2023

The scan was started on June 29, 2023 at 09:37 pm GMT and took 01:22:18 to complete. The scan was run against the following IP addresses:

Not a certified PCI report

IP/DNS Scanned

3.29.26.82
3.29.30.141

The scan option profile used includes:

Scan Settings

| | |
|--|---------------|
| Scanned TCP Ports | Full |
| Scanned UDP Ports | Standard Scan |
| Scan Dead Hosts | Off |
| Load Balancer Detection | Off |
| Password Brute Forcing | Standard |
| Vulnerability Detection | Complete |
| Windows Authentication | Disabled |
| SSH Authentication | Disabled |
| Oracle Authentication | Disabled |
| SNMP Authentication | Disabled |
| Perform 3-way Handshake | Off |
| Overall Performance | Custom |
| Hosts to Scan in Parallel-External Scanner | 15 |
| Hosts to Scan in Parallel-Scanner Appliances | 15 |
| Processes to Run in Parallel-Total | 10 |
| Processes to Run in Parallel-HTTP | 10 |
| Packet (Burst) Delay | Medium |

Advanced Settings

| | |
|---|-------------------|
| Host Discovery | TCP Standard Scan |
| | UDP Standard Scan |
| | ICMP On |
| Ignore RST packets | Off |
| Ignore firewall-generated SYN-ACK packets | Off |
| ACK/SYN-ACK packets during discovery | Send |

Report Summary

| | |
|--------------------|--|
| Company: | PayDart |
| User: | Pavan Kumar |
| Template Title: | Scan Results |
| Active Hosts: | 1 |
| Total Hosts: | 2 |
| Scan Type: | On Demand |
| Scan Status: | Finished |
| Scan Title: | Two IPs |
| Scan Date: | 06/29/2023 at 21:37:50 |
| Reference: | scan/1688074682.61733 |
| Scanner Appliance: | 64.39.111.227 (Scanner 12.14.21-1, Vulnerability Signatures 2.5.803-3) |
| Duration: | 01:22:18 |
| Options: | Payment Card Industry (PCI) Options |
| Target: | 3.29.26.82, 3.29.30.141 |

Summary of Vulnerabilities

| | | | | |
|-----------------------|----|-----------------------|---|-----|
| Vulnerabilities Total | 50 | Average Security Risk |  | 2.0 |
|-----------------------|----|-----------------------|---|-----|

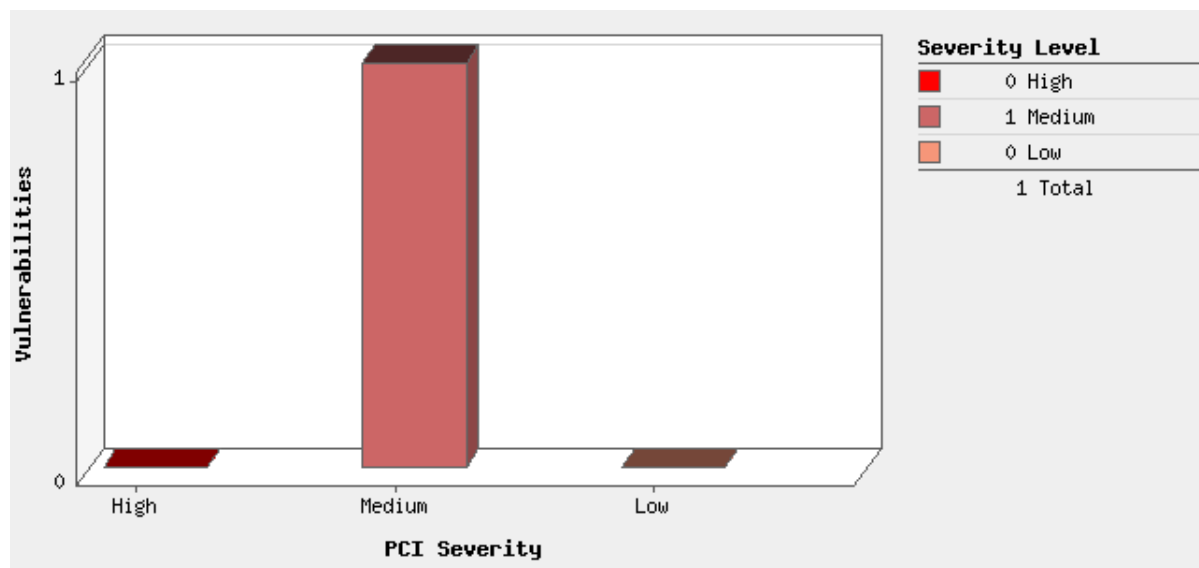
by Severity

| Severity | Confirmed | Potential | Information Gathered | Total |
|----------|-----------|-----------|----------------------|-------|
| 5 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 2 | 2 |
| 2 | 1 | 0 | 6 | 7 |
| 1 | 0 | 0 | 41 | 41 |
| Total | 1 | 0 | 49 | 50 |

by PCI Severity

| PCI Severity | Confirmed | Potential | Total |
|--------------|-----------|-----------|-------|
| High | 0 | 0 | 0 |
| Medium | 1 | 0 | 1 |
| Low | 0 | 0 | 0 |
| Total | 1 | 0 | 1 |

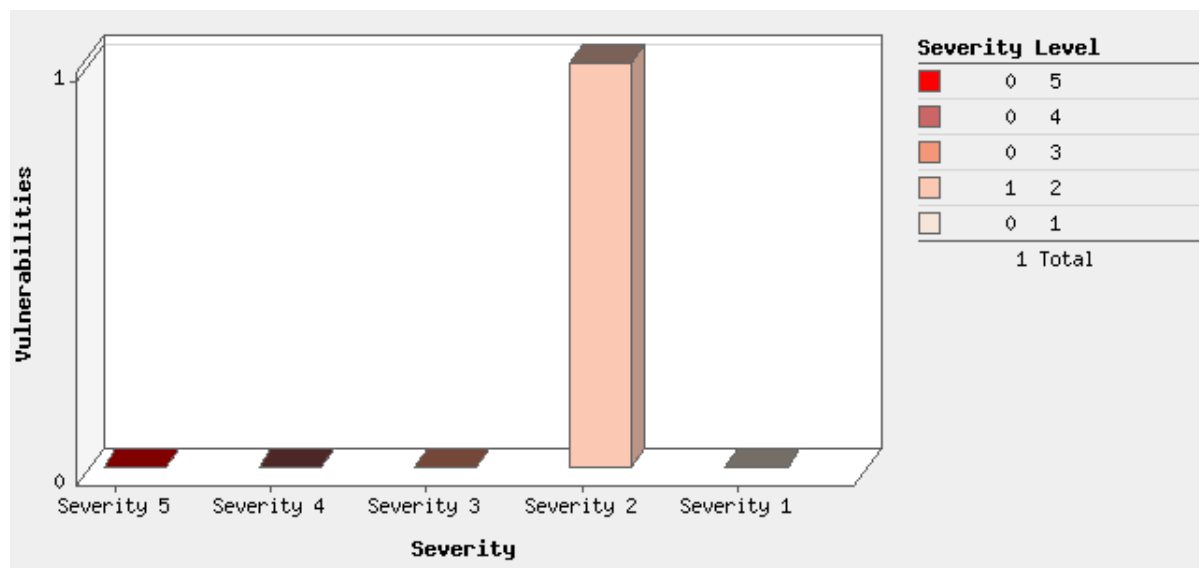
Vulnerabilities by PCI Severity



Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity



Potential Vulnerabilities by Severity

There is no data available

Detailed Results

3.29.26.82 (ec2-3-29-26-82.me-central-1.compute.amazonaws.com,-)

Ubuntu/Linux

Vulnerabilities Total

50

Security Risk

2.0

Compliance Status

FAIL

Vulnerabilities (1)

HTTP Security Header Not Detected

port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity:

■ MED

FAIL

The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score: **5.3** AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS Temporal Score: **4.7** E:U/RL:U/RC:R
Severity: **2** ■ ■ ■ ■
QID: 11827
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/29/2023

THREAT:

This QID reports the absence of the following HTTP headers according to CWE-693: Protection Mechanism Failure:

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.

Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:

This unauthenticated QID looks for the presence of the following HTTP responses:

The Valid directives are as follows:

X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -IkL --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper X-Content-Type-Options (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>) and Strict-Transport-Security (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:

Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:

Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

Strict-Transport-Security HTTP Header missing on port 443.

GET / HTTP/1.0

Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.0 200 OK

Accept-Ranges: bytes

Cache-Control: no-cache, no-store, must-revalidate

Content-Length: 1768

Content-Type: text/html; charset=utf-8

Last-Modified: Mon, 10 Apr 2023 17:31:06 GMT

X-Api-Cattle-Auth: false

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

Date: Thu, 29 Jun 2023 22:23:46 GMT

Connection: keep-alive

Information Gathered (49)

DEFLATE Data Compression Algorithm Used for HTTPS

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 

QID: 42416

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 08/10/2013

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-Encoding: gzip
Content-Type: application/json
Expires: Wed 24 Feb 1982 18:42:00 GMT
X-Api-Cattle-Auth: false
X-Api-Schemas: https://3.29.26.82/meta/schemas
X-Content-Type-Options: nosniff
Date: Thu, 29 Jun 2023 22:14:15 GMT
Content-Length: 1468

_1F_8B_08_00_00_00_00_00_FF_9C_98_Df0_1C)_12_C7_DF_EF_CF_A8g_E4I_E2_D3)7_D2_E9_E48R_B4_BBr_D6_B2_B3_D9_87_D5>0ty_86_0C_08_E8Yy_FF_EF+~u3_8E_07_98<Y_EE_FE|_BF4P_14U_F3_04_EEQ#_AC_81)!_909_AE\$ _10_10_EE-_AC_9F_C0_A2x_805_EC_9C_D3v_BDZ|^_BC_FB_EF_C5_BB_FF_BC_7F_B7_82g_024_F0_1E|&_A0_E9_96K_1A_0C_D6O_F8_C8_1D_AC_DF_BEy_F3_86_80S_8E
X_FF_FB_99_80U_C6_F9_F7_CA_0Ch`_D42`_F0_80_C6_E2_EB#_FD?_B0_FF_1B_D02?_A8A_AB&_C3_F0K_FcN_AA_F9_9DR_0E_08_0C_D4QX_FF_F1_E4_1F)
Ec_D3_97L_8D_9A4_AcAdG/_18uN_E0_05W_E0?_D8_ED'+_FF_02_08_1C_B2_04_0Eo_FD8_1Bj_BF_1Fc^_98_F4_C8_BE_FE_C9_DErE57_01!_E0_FF_9E&_81_80e;_1Ci_CD-_13_A4_B2'_D9L_DAXf_F8_E6_C4zF_BB_99y&9_04_F24_9F_C9_C95_A4_92nqD_E9^]_C9_C3_E5_F1^v_AC_E3_E4v_D7J>_F0_ED_89_C9_1Fw_9Ea_89!_C0_A8_A3BU_F0_19_C0_84_9A_86k_83_03J_C7_A9_A8h<_C8
_D0k'_EB_D0\ 4_EE_93_9F_7FM_1DP_EA_D1mD_8F_F5w_93_C0>_B9_E4_B1_BAOY_A8_AE_9BK_14_B9_A3_95
On_94_E4N_99O_86_EA]S>F_x_1B_E1_D9_E3_0E_B7_DC:_13R_C1_17_B5G_D942_85_C2E_C5_E2_A6_04~_C1Q_0B_EA_F0_03_97_03_97_Edy_19%_D0%
_CD&kf_C7_EcV_87_07nc_FE_AA_DBe+3_0B_BE_F3_EA_F6(_B4MM'_D5_A8_95_C5_D6_11!_D8rJ_86GIG_CE_EEky_E5p_B9J_D8_92L_D0_B1_E1_03e_FBZ_B8
{f_93_18_02_0FH_DDd'+0_03_04_1E_04_A2_FB]_99_BD_D5_94_D5\$ _9E_FBk_E1_08!_85_DAP_F1Q_DA[_A3_0E]^_A8_AD^D_07i_F5_8C_16_FA_CA_A8_B3_B0_18_D1_87_3_EC
_EA_A3_AE_88_B6E_DF#_0C
_9F:np_DCTg_E7_A11AI_D3_A0=_B7W_D2Q_ _D1]4_FCP_F3_9F_C1!_81_04_C4@u+~00=_B3D_DFrO_DC#3X_C9'_0Bi_13l_E5_95_1Bt_86_B3_8A4bc_C2_08_8C_93p_FC%:N_AD_DB_E7;
_08r_0E_D5_BA<_DF/_BC_BA=BCV_AA_01[_CB_EC_99e_85_FD_7F_B7JU.(O_E8@D_BA_9Dx<Uf_1D_FF_7F_9D_8E_94_E3_0F_BC_FE_E5_99_A0_D5p_8F12_DC=^#_B7~_F5b_A4L)
_FF7?S_AB_C1&_0B_9A-XiQ_CE_A1_18_EFV_CE_1E_B3_FF_ADQ_DF_90_B9_E6I-F_D3_C1_BB_EBhP_9C_DF_93c_FD_80[_F03_F8_80_06e-_EF_95_8CWp_C9_B8_AE_D5-_05_E2_F90_87_9E_8A%_A1_C7_15K_A9_AFW_A5<W_A5_BAOY_A8_9A_15K_E2_8A_8A%=_E9_ABX_12_FC_B2bl_8F?
_C7_CB&I3oO[Fg]_F69_AbVl_9A_13_B5Jz_DB_94_87_EE_82J_B6C_F3_9BE_F39_1CNF]5_EF%_C1d_D1_C8#_01_01_B3_C7_ABa_A8_8A_F7H#_11_E8_DE_DB
(4_07_CE_F0W_DD_18u_8F_FB_F7_D6FX_E9bD_EF_F1h_1D_8E?_8D[y_FF_E4_10P_1EQ_DF[_89_8EIX.s_BD#_0BM_8C_A5_A3h_D4_AE_1E_99_8B_D5_D3=
Y_B4C_E7_AA_C10_03_CD_EE_CD_C33A_CF]5k_A7G_C8_E0!_83_8B_B6-
t)9_E6_A5_F0Qu_1A_8Bo_CF_E99_D3_DDz_A2_E1_CC_B5_F2_F9_8D_A7_E6)n_9Bu_B8_EF_E4mf_H:b_A3~_CD_C2_02%_A0_FD_F7Y_87_D2]Ub_1A:_E4_8B_E2_90_14_F5_C0-
_16_A3_16_90%_E6_94_A1[_BC_16_D4_D6*_E3_FCA_g_EF_D6Y_FAC?8_A4,wj_F3_D3_EB_F37_DF_?_B1_F4.AC_C4jr_1D_D3_04hOm9_8B_8F_EBJZ_AB%
_0B_8Dg7_D4rv5_B9_F6_BD_B6
((_01_86&%_F5_F6]_B6:~82)_BF_E9K_AF_1B_DA_F1_95_11Di_FC_B5_C3[_F9_B3_Dat_A8_8C_92_DF<H^_A08*y_k_0F_B2*_A26_F6_07_03j_A1_1EC_CF_D0_16_16_81A_DA;
d_CA_0C_1DBiMB_0C_8A_ED_D1_F4_FC_904_CB_83_E2_F8_17_A5_9D2_FCo_Df^_89]5MNY_E6C_AbM_B6_08_B5_1Ah!\$_C0_E5_D6'_F5_EcF_93_85\$ _F0_Adg_A7_D2.
_CD9L_F8_D0_1F_8F_8B_E8(2_97_C7_D7_E7_C4_E8*[_11_AD_CB_8B_8Fg_EF_D0_A2]m_AF_96_B7_AD_0E_F6[_BF_A5_93_]_C2_FDq_C5_98_9A_A4k_94_16_AFY_069_8D_F2_F9_AE-
_FC_ED_EE_DC_9D_B1v_97_F7_E5_E5_D5t(-_1F_DB^_EF'_16e_A1w_EAP_ABIU_BA#_BA_1DN_B6_AB_E7X-[_D1y_A4g_C9_E3u_8AZpF_BB_92PbS_16J_FF_B9_D8_F2_FA:_BE_EB,
_172V_C8_1A_17_FBr_D1_D9_CEpL_82_B0Z
_94_C6?_10_A1'_E22=N_BDY_B7_CD_98_F9_D9_A1[_1A4_BDg_A0_88]_EB_A8_C3_87tl_05@_86S_04_B4_8B_9FYXT_EC_BEu_14_8Av_1C_90_85]
_A5d_FA_F3_F9_FF_04_00_00_FF_FF_04u_11_CA_BC_1B

HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-Encoding: gzip
Content-Type: application/json
Expires: Wed 24 Feb 1982 18:42:00 GMT
X-Api-Cattle-Auth: false
X-Api-Schemas: https://3.29.26.82/meta/schemas
X-Content-Type-Options: nosniff
Date: Thu, 29 Jun 2023 22:14:22 GMT
Content-Length: 1468

_1F_8B_08_00_00_00_00_00_FF_9C_98_Df0_1C)_12_C7_DF_EF_CF_A8g_E4I_E2_D3)7_D2_E9_E48R_B4_BBr_D6_B2_B3_D9_87_D5>0ty_86_0C_08_E8Yy_FF_EF+~u3_8E_07_98<Y_EE_FE|_BF4P_14U_F3_04_EEQ#_AC_81)!_909_AE\$ _10_10_EE-_AC_9F_C0_A2x_805_EC_9C_D3v_BDZ|^_BC_FB_EF_C5_BB_FF_BC_7F_B7_82g_024_F0_1E|&_A0_E9_96K_1A_0C_D6O_F8_C8_1D_AC_DF_BEy_F3_86_80S_8E
X_FF_FB_99_80U_C6_F9_F7_CA_0Ch`_D42`_F0_80_C6_E2_EB#_FD?_B0_FF_1B_D02?_A8A_AB&_C3_F0K_FcN_AA_F9_9DR_0E_08_0C_D4QX_FF_F1_E4_1F)
Ec_D3_97L_8D_9A4_AcAdG/_18uN_E0_05W_E0?_D8_ED'+_FF_02_08_1C_B2_04_0Eo_FD8_1Bj_BF_1Fc^_98_F4_C8_BE_FE_C9_DErE57_01!_E0_FF_9E&_81_80e;_1Ci_CD-_13_A4_B2'_D9L_DAXf_F8_E6_C4zF_BB_99y&9_04_F24_9F_C9_C95_A4_92nqD_E9^]_C9_C3_E5_F1^v_AC_E3_E4v_D7J>_F0_ED_89_C9_1Fw_9Ea_89!_C0_A8_A3BU_F0_19_C0_84_9A_86k_83_03J_C7_A9_A8h<_C8
_D0k'_EB_D0\ 4_EE_93_9F_7FM_1DP_EA_D1mD_8F_F5w_93_C0>_B9_E4_B1_BAOY_A8_AE_9BK_14_B9_A3_95
On_94_E4N_99O_86_EA]S>F_x_1B_E1_D9_E3_0E_B7_DC:_13R_C1_17_B5G_D942_85_C2E_C5_E2_A6_04~_C1Q_0B_EA_F0_03_97_03_97_Edy_19%_D0%
_CD&kf_C7_EcV_87_07nc_FE_AA_DBe+3_0B_BE_F3_EA_F6(_B4MM'_D5_A8_95_C5_D6_11!_D8rJ_86GIG_CE_EEky_E5p_B9J_D8_92L_D0_B1_E1_03e_FBZ_B8
{f_93_18_02_0FH_DDd'+0_03_04_1E_04_A2_FB]_99_BD_D5_94_D5\$ _9E_FBk_E1_08!_85_DAP_F1Q_DA[_A3_0E]^_A8_AD^D_07i_F5_8C_16_FA_CA_A8_B3_B0_18_D1_87_3_EC
_EA_A3_AE_88_B6E_DF#_0C
_9F:np_DCTg_E7_A11AI_D3_A0=_B7W_D2Q_ _D1]4_FCP_F3_9F_C1!_81_04_C4@u+~00=_B3D_DFrO_DC#3X_C9'_0Bi_13l_E5_95_1Bt_86_B3_8A4bc_C2_08_8C_93p_FC%:N_AD_DB_E7;
_08r_0E_D5_BA<_DF/_BC_BA=BCV_AA_01[_CB_EC_99e_85_FD_7F_B7JU.(O_E8@D_BA_9Dx<Uf_1D_FF_7F_9D_8E_94_E3_0F_BC_FE_E5_99_A0_D5p_8F12_DC=^#_B7~_F5b_A4L)
_FF7?S_AB_C1&_0B_9A-XiQ_CE_A1_18_EFV_CE_1E_B3_FF_ADQ_DF_90_B9_E6I-F_D3_C1_BB_EBhP_9C_DF_93c_FD_80[_F03_F8_80_06e-_EF_95_8CWp_C9_B8_AE_D5-_05_E2_F90_87_9E_8A%_A1_C7_15K_A9_AFW_A5<W_A5_BAOY_A8_9A_15K_E2_8A_8A%=_E9_ABX_12_FC_B2bl_8F?_C7_CB&I3oO[Fg]_F69_AbVl
_9A_13_B5Jz_DB_94_87_EE_82J_B6C_F3_9BE_F39_1CNF]5_EF%_C1d_D1_C8#_01_01_B3_C7_ABa_A8_8A_F7H#_11_E8_DE_DB
(4_07_CE_F0W_DD_18u_8F_FB_F7_D6FX_E9bD_EF_F1h_1D_8E?_8D[y_FF_E4_10P_1EQ_DF[_89_8EIX.s_BD#_0BM_8C_A5_A3h_D4_AE_1E_99_8B_D5_D3=
Y_B4C_E7_AA_C10_03_CD_EE_CD_C33A_CF]5k_A7G_C8_E0!_83_8B_B6-
t)9_E6_A5_F0Qu_1A_8Bo_CF_E99_D3_DDz_A2_E1_CC_B5_F2_F9_8D_A7_E6)n_9Bu_B8_EF_E4mf_H:b_A3~_CD_C2_02%_A0_FD_F7Y_87_D2]Ub_1A:_E4_8B_E2_90_14_F5_C0-
_16_A3_16_90%_E6_94_A1[_BC_16_D4_D6*_E3_FCA_g_EF_D6Y_FAC?8_A4,wj_F3_D3_EB_F37_DF_?_B1_F4.AC_C4jr_1D_D3_04hOm9_8B_8F_EBJZ_AB%
_0B_8Dg7_D4rv5_B9_F6_BD_B6
((_01_86&%_F5_F6]_B6:~82)_BF_E9K_AF_1B_DA_F1_95_11Di_FC_B5_C3[_F9_B3_Dat_A8_8C_92_DF<H^_A08*y_k_0F_B2*_A26_F6_07_03j_A1_1EC_CF_D0_16_16_81A_DA;
d_CA_0C_1DBiMB_0C_8A_ED_D1_F4_FC_904_CB_83_E2_F8_17_A5_9D2_FCo_Df^_89]5MNY_E6C_AbM_B6_08_B5_1Ah!\$_C0_E5_D6'_F5_EcF_93_85\$ _F0_Adg_A7_D2.
_CD9L_F8_D0_1F_8F_8B_E8(2_97_C7_D7_E7_C4_E8*[_11_AD_CB_8B_8Fg_EF_D0_A2]m_AF_96_B7_AD_0E_F6[_BF_A5_93_]_C2_FDq_C5_98_9A_A4k_94_16_AFY_069_8D_F2_F9_AE-
_FC_ED_EE_DC_9D_B1v_97_F7_E5_E5_D5t(-_1F_DB^_EF'_16e_A1w_EAP_ABIU_BA#_BA_1DN_B6_AB_E7X-[_D1y_A4g_C9_E3u_8AZpF_BB_92PbS_16J_FF_B9_D8_F2_FA:_BE_EB,
_172V_C8_1A_17_FBr_D1_D9_CEpL_82_B0Z
_94_C6?_10_A1'_E22=N_BDY_B7_CD_98_F9_D9_A1[_1A4_BDg_A0_88]_EB_A8_C3_87tl_05@_86S_04_B4_8B_9FYXT_EC_BEu_14_8Av_1C_90_85]
_A5d_FA_F3_F9_FF_04_00_00_FF_FF_04u_11_CA_BC_1B


Content-Security-Policy HTTP Security Header Not Detected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **3** 
QID: 48001
Category: Information gathering
CVE ID: -
Vendor Reference: [Content-Security-Policy](#)
Bugtraq ID: -
Last Update: 03/11/2019

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:

This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

RESULT:


Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.0
Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **2** 
QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/25/2023

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service

maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

RESULT:

| Operating System | Technique | ID |
|------------------|--------------------|----------|
| Ubuntu/Linux | TCP/IP Fingerprint | U7254:80 |


Web Server HTTP Protocol Versions

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 45266
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 04/24/2017

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

RESULT:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1


Connection Error Occurred During Web Application Scan

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 150018
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/16/2021

THREAT:

The following are some of the possible reasons for the timeouts or connection errors:

A disturbance in network connectivity between the scanner and the web application occurred.
The web server or application server hosting the application was taken down in the midst of a scan.

The web application experienced an overload, possibly due to load generated by the scan.
An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

IMPACT:

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

RESULT:

Total number of unique links that encountered connection errors: 106

Links with highest number of connection errors:

- 65 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/db/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/logs/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/upload/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.tar.gz>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/build.xml>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/reports/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/CHANGELOG>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/WVS/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/sendRequest.jsp>
- 1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/_core/
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/private/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.tar.bz2>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/web/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/service/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/cache/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/saved/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/web.config>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/administration/>
- 1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/DisplayEnroll_style.jsp
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/admin/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/test.php>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/css/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/php.ini>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/include/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/zip/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/external/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/core/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/includes/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/INSTALL>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/backup/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/webmail/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/lib/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/info.php>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/documents/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/test.jsp>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/image/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/test/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/BUGS>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/WebService/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.old>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.inc>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/users/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/download/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/tmp/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/tools/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/internet/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/extranet/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/common/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.tar>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/manager/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/>
- 1 <https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/bin/>

```

1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/uploads/
1 https://ec2-3-29-26-82.me-central-1.compu
te.amazonaws.com/phpMyAdmin/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/php/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.git/config
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/history/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/images/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/test.aspx
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/root/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.zip
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/roles/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/WSDL/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/phpinfo.php
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/wsdl/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/SERVICE/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/java/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.gz
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/js/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/data/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/export/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.bak
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/imports/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/misc/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/sources/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.orig
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/CHANGELOG.txt
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/www/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/admin.aspx
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/admin.jsp
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/modules/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/
functions/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.svn/entries
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/jsp/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/package.json
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/install/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/config/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/ws/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/classes/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/admin.php
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/temp/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/plugins/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/files/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/CVS/Entries
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/ChangeLog.txt
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/README.txt
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/docs/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/security/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/mirror/

```

Phase wise summary of timeout and connection errors encountered:

```

ePhaseCrawl           :      0      2
ePhaseWSDirectoryPathTests :      0      9
ePhaseHeaderTests     :      0     63
ePhaseShellShock      :      0      1
ePhasePathTests       :      0     95

```


Web Server HTTP Protocol Versions

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **2** 

QID: 45266

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 04/24/2017

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

RESULT:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1


Connection Error Occurred During Web Application Scan

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 150018
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/16/2021

THREAT:

The following are some of the possible reasons for the timeouts or connection errors:

- A disturbance in network connectivity between the scanner and the web application occurred.
- The web server or application server hosting the application was taken down in the midst of a scan.
- The web application experienced an overload, possibly due to load generated by the scan.
- An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
- A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
- Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

IMPACT:

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

RESULT:

Total number of unique links that encountered connection errors: 7
Links with highest number of connection errors:
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/lh319a980sdS.html
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/..
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/crossdomain.xml
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/icons/small/
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/.
1 https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/src/


Phase wise summary of timeout and connection errors encountered:
ePhaseCrawl : 0 7

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 82063
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/29/2007

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:


Based on TCP timestamps obtained via port 80, the host's uptime is 47 days, 22 hours, and 39 minutes. The TCP timestamps from the host are in units of 1 milliseconds.

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 6
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/04/2018

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:


| IP address | Host name |
|------------|---|
| 3.29.26.82 | ec2-3-29-26-82.me-central-1.compute.amazonaws.com |

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:


| Hops | IP | Round Trip Time | Probe | Port |
|------|----------------|-----------------|-------|------|
| 1 | 64.39.111.4 | 0.26ms | ICMP | |
| 2 | *.*.* | 0.00ms | Other | 80 |
| 3 | 154.24.30.65 | 0.99ms | ICMP | |
| 4 | 154.54.31.109 | 1.33ms | ICMP | |
| 5 | 154.54.43.69 | 2.13ms | ICMP | |
| 6 | 154.54.44.138 | 16.59ms | ICMP | |
| 7 | 154.54.41.146 | 26.66ms | ICMP | |
| 8 | 154.54.5.90 | 37.97ms | ICMP | |
| 9 | 154.54.42.166 | 49.78ms | ICMP | |
| 10 | 154.54.6.222 | 56.41ms | ICMP | |
| 11 | 154.54.26.130 | 66.95ms | ICMP | |
| 12 | 66.28.4.238 | 70.32ms | ICMP | |
| 13 | 154.54.82.33 | 132.22ms | ICMP | |
| 14 | 130.117.51.74 | 132.59ms | ICMP | |
| 15 | 149.11.173.122 | 132.10ms | ICMP | |
| 16 | *.*.* | 0.00ms | Other | 80 |
| 17 | *.*.* | 0.00ms | Other | 80 |
| 18 | *.*.* | 0.00ms | Other | 80 |
| 19 | *.*.* | 0.00ms | Other | 80 |
| 20 | *.*.* | 0.00ms | Other | 80 |
| 21 | *.*.* | 0.00ms | Other | 80 |
| 22 | 3.29.26.82 | 252.92ms | TCP | 80 |

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45004
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/15/2013

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

RESULT:


The network handle is: NET-3-28-0-0-1
Network description:
Amazon Data Services UAE AMAZON-DXB

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45005
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/27/2013

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

RESULT:


The ISP network handle is: COGENT-149-11-16
ISP Network description:
PSINet, Inc.

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/27/2020

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:


| Host Name | Source |
|---|--------|
| ec2-3-29-26-82.me-central-1.compute.amazonaws.com | FQDN |

Host Scan Time - Scanner

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/15/2022

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 4898 seconds

Start time: Thu, Jun 29 2023, 21:39:17 GMT


End time: Thu, Jun 29 2023, 23:00:55 GMT

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45426
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/24/2020

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

RESULT:


| Protocol | Port | Time |
|----------|------|---------|
| TCP | 80 | 3:51:24 |
| TCP | 443 | 8:12:18 |

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82040
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2003

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

- Echo Request (to trigger Echo Reply)
- Timestamp Request (to trigger Timestamp Reply)
- Address Mask Request (to trigger Address Mask Reply)
- UDP Packet (to trigger Port Unreachable Reply)
- IP Packet with Protocol \geq 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.


| ICMP Reply Type | Triggered By | Additional Information |
|--------------------------------|--------------|------------------------|
| Time Exceeded (type=11 code=0) | (Various) | Time Exceeded |

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 82045
 Category: TCP/IP
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 11/19/2004

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

RESULT:


Average change between subsequent TCP initial sequence numbers is 1120816550 with a standard deviation of 576530478. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4994 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 82046
 Category: TCP/IP
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 07/27/2006

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

RESULT:


IP ID changes observed (network order) for port 80: 0
 Duration: 31 milli seconds

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (<http://www.cert.org>).

RESULT:


| Port | IANA Assigned Ports/Services | Description | Service Detected | OS On Redirected Port |
|------|------------------------------|----------------------------|------------------|-----------------------|
| 80 | www-http | World Wide Web HTTP | http | |
| 443 | https | http protocol over TLS/SSL | http over ssl | |

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 04/22/2019

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports are probed.

1-79,81-442,444-6128,6130-65535


Links Rejected By Crawl Scope or Exclusion List

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150020
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/07/2022

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:


Scan Diagnostics

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Ineffective Session Protection. no tests enabled.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 1 minutes duration.
No links were discovered during the crawl phase.
Duration of Crawl Time: 82.00 (seconds)
Duration of Test Phase: 0.00 (seconds)
Total Scan Time: 82.00 (seconds)

Total requests made: 7
Average server response time: 0.00 seconds

Average browser load time: 0.00 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found


Links Crawled

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/27/2020

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 82.00
Number of links: 0
(This number excludes form requests and links re-requested during authentication.)

No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.


List of Web Directories

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86672
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/10/2004

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

RESULT:

| Directory | Source |
|-----------------------|-------------|
| /assets/ | brute force |
| /assets/images/ | brute force |
| /api/ | brute force |
| /wordpress// | brute force |
| /assets/ | web page |
| /assets/images/ | web page |
| /assets/images/logos/ | web page |
| /dashboard/ | web page |
| /dashboard/_nuxt/ | web page |


Content of robots.txt found during VM Scan

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 45221
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/05/2014

THREAT:

The content of the robots.txt file appears in the Results section.

RESULT:

```
# +++++?+?+?~=====+??+
# ++++++?+8,~=-O=-+=====D????+
# ++++++N~=-~+7=====+??+
# ++++++Z~-I$~=-Z+=====8?++++
# ++++++?Z~-MMMMMMMM~-I$=====+++++
# ++++++?8=-MMMMMMMM,MM7:=~Z$=====I?++++
# ++++++??=-MMMMMM,MMMMN+~ZI=====D?++++
# ++++++O~?MMMMM,MM,MMMMMMMD=-I8Z=====??++++
# ++++++?~=-MMMMMM,MMM$,MMMMMMMMMM~=-O?++++
# ++++++?~-MMMMMM,MMMMMMMMMMMMMMO~=-??+?++
# ++++++?+8=-MMMMM,MMMMMMMMMMMMMMMMMN~-O?++++
# ++++++?~-MMMMM,MMN,MM,MMM~?+?++
# ++++++O=-ZMMM,MM$,MMMM,MMMMI=-$++?+
# ++++++8MM$,MMMM~,MMMMM=-D++?+
# ++++++?+~=-IMMMMMMMMMMMMMMM,MMMMMO=I+?+
# ++++++D=-8MMMMMMMMMM,MMMMMM~,?++++
# ++++++?~$~-IMMMMMMM?,MMMMM~-?+?++
# ++++++?8=====Z:~IMMMMN,8MMMMMM=-+?++++
# ++++++D-8+?=$7~IMMMMMMMMMMM~-8?++++
# ++++++?+?+D,?,Z+=OZ=-8??+?++++
# ++++++?+?+?+?+D,?,Z+=OZ=-8??+?++++
# ++++++VJF82+=,Z,=.O,.,,I87~=====+?++++
# ++++++$8=-~7=+,I,.,,Z,.,,D,.,.?.7==8?+
++++
# ++++?7$~=-?=,8:,+...-O?,Z,=7+?++++
# ++$:-=D,.,N,.,I,.,DZ+,.,=-~+?++++
# ~~~~~,.,D,.,Z,.,8,.,=I?+?++++
# ==~~~~M=====D,.,-OZ-,.,8=8+?+?++++
# ~~~~~D=+=====Z:8,.,.,:++?+?+?++++
# ~~~~~I+======B$,Z,.,-D===?$+?+?++++
# ~~~~~-O=====+=====O~=-:++++
# ~~~~~-O?+=====8+?++++
# ~~~~~-78$+=====Z8+~$++++
# ~:-~=-?+?++++
# =-7:~=-I+?++++
# ==+O~=-++++
# ,-:+=-,=-++++
# =====8~=-+?++++
User-Agent: *
Disallow: /
```

HTTP Public-Key-Pins Security Header Not Detected

port 443/tcp

PCI COMPLIANCE STATUS



VULNERABILITY DETAILS

| | |
|-------------------|-----------------------|
| Severity: | 1 |
| QID: | 48002 |
| Category: | Information gathering |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Last Update: | 07/12/2021 |

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

RESULT:


HTTP Response Method and Header Information Collected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48118
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/20/2020

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 443.

GET / HTTP/1.0
Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

HTTP/1.0 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: application/json
Expires: Wed 24 Feb 1982 18:42:00 GMT
X-Api-Cattle-Auth: false
X-Api-Schemas: https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/schemas
X-Content-Type-Options: nosniff
Date: Thu, 29 Jun 2023 22:13:27 GMT


Referrer-Policy HTTP Security Header Not Detected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48131
Category: Information gathering
CVE ID: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Last Update: 01/18/2023

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

RESULT:

Referrer-Policy HTTP Header missing on 443 port.
GET / HTTP/1.0
Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com


cAdvisor (Container Advisor) Detected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48228
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Last Update: 12/22/2022

THREAT:

cAdvisor (Container Advisor) provides container users an understanding of the resource usage and performance characteristics of their running containers. It is a running daemon that collects, aggregates, processes, and exports information about running containers.

QID Detection Logic:(Unauthenticated)

This QID sends a GET request to check if the authentication is enabled by querying the following endpoints /api/v1.3/./api/v2.0/

RESULT:

cAdvsior Detected on port 443 over TCP.


Links Rejected By Crawl Scope or Exclusion List

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150020
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/07/2022

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:


Scan Diagnostics

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <http://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/> fetched. Status code:302, Content-Type:text/html, load time:511 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 10 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 3 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 21 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
WebCgiOobTests: no test enabled
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 1 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 126 requests, 118 seconds. Completed 126 requests of 130 estimated requests (96.9231%). XSS optimization removed 29 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 2 requests, 11 seconds. Completed 2 requests of 1 estimated requests (200%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
 Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
 Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)
 Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)
 Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.
 Tomcat Vuln manipulation no tests enabled.
 Time based path manipulation no tests enabled.
 Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 0) + files:(10 x 0) + directories:(92 x 1) + paths:(9 x 1) = total (101)
 Batch #5 Path manipulation: estimated time < 1 minute (114 tests, 1 inputs)
 Batch #5 Path manipulation: 114 vulnsigs tests, completed 100 requests, 130 seconds. Completed 100 requests of 101 estimated requests (99.0099%). All tests completed.
 WebCgiHrsTests: no test enabled
 Batch #5 WebCgiGeneric: estimated time < 1 minute (319 tests, 1 inputs)
 Batch #5 WebCgiGeneric: 319 vulnsigs tests, completed 1 requests, 1 seconds. Completed 1 request s of 398 estimated requests (0.251256%). All tests completed.
 Duration of Crawl Time: 36.00 (seconds)
 Duration of Test Phase: 283.00 (seconds)
 Total Scan Time: 319.00 (seconds)

Total requests made: 400
 Average server response time: 0.29 seconds

Average browser load time: 0.30 seconds
 Scan launched using PCI WAS combined mode.
 HTML form authentication unavailable, no WEBAPP entry found


Links Crawled

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 150009
 Category: Web Application
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 07/27/2020

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

RESULT:

Duration of crawl phase (seconds): 36.00
 Number of links: 1
 (This number excludes form requests and links re-requested during authentication.)

<http://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/>


List of Web Directories

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86672
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/10/2004

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

RESULT:

| Directory | Source |
|---|----------|
| /\$%7B%28%22QualysQID%22+%2213251%22%29%7D/ | web page |
| /%22%3E%3Cscript%3Ealert%28document.domain%29%3C/ | web page |
| /admin/ | web page |
| /help/ | web page |
| /install/ | web page |
| /secure/ | web page |
| /crx/ | web page |
| /crx/explorer/ | web page |
| /crx/explorer/browser/ | web page |


Web Server Supports HTTP Request Pipelining

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86565
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/23/2005

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker, it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

RESULT:

GET / HTTP/1.1
Host:3.29.26.82:80

GET /Q_Evasive/ HTTP/1.1
Host:3.29.26.82:80

HTTP/1.1 302 Found
Content-Type: text/html; charset=utf-8
Location: https://3.29.26.82:443/
Date: Thu, 29 Jun 2023 22:13:06 GMT
Content-Length: 46

Found (https://3.29.26.82:443/).

HTTP/1.1 302 Found
Content-Type: text/html; charset=utf-8
Location: https://3.29.26.82:443/Q_Evasive/
Date: Thu, 29 Jun 2023 22:13:06 GMT
Content-Length: 56

Found (https://3.29.26.82:443/Q_Evasive/).


Default Web Page

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 12230
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/16/2019

THREAT:

The Result section displays the default Web page for the Web server.

RESULT:

GET / HTTP/1.0
Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

Found (https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/).


HTTP Response Method and Header Information Collected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48118
Category: Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/20/2020

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 80.

GET / HTTP/1.0

Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

HTTP/1.0 302 Found
Content-Type: text/html; charset=utf-8
Location: https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/
Date: Thu, 29 Jun 2023 21:46:52 GMT
Content-Length: 81
Connection: keep-alive


Referrer-Policy HTTP Security Header Not Detected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48131
Category: Information gathering
CVE ID: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Last Update: 01/18/2023

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/> (<https://www.w3.org/TR/referrer-policy/>)
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy> (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>)

RESULT:

Referrer-Policy HTTP Header missing on 80 port.
GET / HTTP/1.0
Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com


SSL Session Caching Information

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38291
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/19/2020

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

RESULT:

TLSv1.2 session caching is enabled on the target.


SSL Certificate will expire within next six months

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38600
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/29/2016

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULT:

Certificate #0 CN=rancher.paydart.co The certificate will expire within six months: Aug 13 19:29:38 2023 GMT


Secure Sockets Layer (SSL) Certificate Transparency Information

port 443/tcp over SSL

PCI COMPLIANCE STATUS



VULNERABILITY DETAILS

Severity: 1 
QID: 38718
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/08/2021

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

RESULT:

| Source | Validated | Name | URL | ID | Time |
|----------------|-----------|-----------------------|-----------|---|---------------------------------|
| Certificate #0 | | CN=rancher.paydart.co | | | |
| Certificate | no | (unknown) | (unknown) | b73efb24df9c4dba75f239c5ba58f46c5dfc42cf7a9f35c49e1d098125edb499 | Thu 01 Jan 1970 12:00:00 AM GMT |
| Certificate | no | (unknown) | (unknown) | e83ed0da3ef5063532e75728bc896bc903d3cb d1116beceb69e1777d6d06bd6e | Thu 01 Jan 1970 12:00:00 AM GMT |

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 [Progress bar]
QID: 42350
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/21/2016

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client.

RESULT:

TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 [Progress bar]
QID: 38597
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/12/2021

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior.


RESULT:

Table with 2 columns: my version, target version. Rows include versions 0304, 0399, 0400, 0499, all with 'rejected' target responses.

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 38116
 Category: General remote services
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 05/24/2016

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

RESULT:


| CIPHER | KEY-EXCHANGE | AUTHENTICATION | MAC | ENCRYPTION(KEY-STRENGTH) | GRADE |
|-------------------------------|--------------------|----------------|-----|-----------------------------|--------|
| SSLv2 PROTOCOL IS DISABLED | | | | | |
| SSLv3 PROTOCOL IS DISABLED | | | | | |
| TLSv1 PROTOCOL IS DISABLED | | | | | |
| TLSv1.1 PROTOCOL IS DISABLED | | | | | |
| TLSv1.2 PROTOCOL IS ENABLED | | | | | |
| TLSv1.2 | COMPRESSION METHOD | None | | | |
| ECDHE-ECDSA-AES128-GCM-SHA256 | ECDH | ECDSA | | AEAD AESGCM(128) | MEDIUM |
| ECDHE-ECDSA-AES256-GCM-SHA384 | ECDH | ECDSA | | AEAD AESGCM(256) | HIGH |
| ECDHE-RSA-AES128-GCM-SHA256 | ECDH | RSA | | AEAD AESGCM(128) | MEDIUM |
| ECDHE-ECDSA-CHACHA20-POLY1305 | ECDH | ECDSA | | AEAD CHACHA20/POLY1305(256) | HIGH |
| TLSv1.3 PROTOCOL IS ENABLED | | | | | |

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 38704
 Category: General remote services
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 02/01/2023

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

RESULT:

| CIPHER | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|-------------------------------|-------|-----------|----------|----------------|--------------------|------------------|
| TLSv1.2 | | | | | | |
| ECDHE-ECDSA-AES256-GCM-SHA384 | ECDHE | x25519 | 256 | yes | 128 | low |
| ECDHE-ECDSA-AES256-GCM-SHA384 | ECDHE | secp384r1 | 384 | yes | 192 | low |
| ECDHE-ECDSA-AES256-GCM-SHA384 | ECDHE | secp256r1 | 256 | yes | 128 | low |
| ECDHE-ECDSA-CHACHA20-POLY1305 | ECDHE | x25519 | 256 | yes | 128 | low |
| ECDHE-ECDSA-CHACHA20-POLY1305 | ECDHE | secp384r1 | 384 | yes | 192 | low |
| ECDHE-ECDSA-CHACHA20-POLY1305 | ECDHE | secp256r1 | 256 | yes | 128 | low |
| ECDHE-RSA-AES128-GCM-SHA256 | ECDHE | x25519 | 256 | yes | 128 | low |
| ECDHE-RSA-AES128-GCM-SHA256 | ECDHE | secp384r1 | 384 | yes | 192 | low |
| ECDHE-RSA-AES128-GCM-SHA256 | ECDHE | secp256r1 | 256 | yes | 128 | low |
| ECDHE-RSA-AES128-GCM-SHA256 | ECDHE | secp521r1 | 521 | yes | 260 | low |
| ECDHE-ECDSA-AES128-GCM-SHA256 | ECDHE | x25519 | 256 | yes | 128 | low |
| ECDHE-ECDSA-AES128-GCM-SHA256 | ECDHE | secp384r1 | 384 | yes | 192 | low |
| ECDHE-ECDSA-AES128-GCM-SHA256 | ECDHE | secp256r1 | 256 | yes | 128 | low |
| TLSv1.3 | | | | | | |

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties port 443/tcp over SSL

PCI COMPLIANCE STATUS



VULNERABILITY DETAILS

Severity: 1

QID: 38706

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 06/09/2021

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to

TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

RESULT:

| NAME | STATUS |
|-------------------------------|--------|
| TLSv1.2 | |
| Extended Master Secret | no |
| Heartbeat | no |
| Cipher priority controlled by | server |
| OCSP stapling | no |
| SCT extension | no |
| TLSv1.3 | |
| Heartbeat | no |
| OCSP stapling | no |
| SCT extension | no |


SSL Certificate - Information

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 86002
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/07/2020

THREAT:

SSL certificate information is provided in the Results section.

RESULT:

| NAME | VALUE |
|-------------------------|---|
| (0)CERTIFICATE 0 | |
| (0)Version | 3 (0x2) |
| (0)Serial Number | 03:47:ed:6f:9f:23:29:dd:71:d0:c1:9e:85:31:21:e1:83:d3 |
| (0)Signature Algorithm | sha256WithRSAEncryption |
| (0)ISSUER NAME | |
| countryName | US |
| organizationName | Let's Encrypt |
| commonName | R3 |
| (0)SUBJECT NAME | |
| commonName | rancher.paydart.co |
| (0)Valid From | May 15 19:29:39 2023 GMT |
| (0)Valid Till | Aug 13 19:29:38 2023 GMT |
| (0)Public Key Algorithm | id-ecPublicKey |
| (0)EC Public Key | |
| (0) | Public-Key: (256 bit) |

| | |
|-----|---|
| (0) | pub: |
| (0) | 04:22:6b:b4:3b:60:06:72:e0:7d:28:5d:f5:04:52: |
| (0) | 6c:0a:20:bd:64:1f:94:bb:84:7f:b7:47:ff:75:81: |
| (0) | 2f:58:27:d3:a7:10:2d:c8:10:e4:82:4e:e8:32:61: |
| (0) | 5c:22:8c:98:71:b5:83:c2:e1:dc:24:5e:27:04:c0: |
| (0) | 34:e1:0a:1b:7e |
| (0) | ASN1 OID: prime256v1 |
| (0) | NIST CURVE: P-256 |
| (0) | X509v3 EXTENSIONS |
| (0) | X509v3 Key Usage critical |
| (0) | Digital Signature |
| (0) | X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication |
| (0) | X509v3 Basic Constraints critical |
| (0) | CA:FALSE |
| (0) | X509v3 Subject Key Identifier 14:93:A7:89:12:3F:28:7F:70:75:27:D8:D0:27:C2:E7:04:A2:89:BF |
| (0) | X509v3 Authority Key Identifier keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 |
| (0) | Authority Information Access OCSP - URL:http://r3.o.lencr.org |
| (0) | CA Issuers - URI:http://r3.i.lencr.org/ |
| (0) | X509v3 Subject Alternative Name DNS:rancher.paydart.co |
| (0) | X509v3 Certificate Policies Policy: 2.23.140.1.2.1 |
| (0) | Policy: 1.3.6.1.4.1.44947.1.1.1 |
| (0) | CPS: http://cps.letsencrypt.org |
| (0) | CT Precertificate SCTs Signed Certificate Timestamp: |
| (0) | Version : v1 (0x0) |
| (0) | Log ID : B7:3E:FB:24:DF:9C:4D:BA:75:F2:39:C5:BA:58:F4:6C: |
| (0) | 5D:FC:42:CF:7A:9F:35:C4:9E:1D:09:81:25:ED:B4:99 |
| (0) | Timestamp : May 15 20:29:39.639 2023 GMT |
| (0) | Extensions: none |
| (0) | Signature : ecdsa-with-SHA256 |
| (0) | 30:45:02:20:39:1C:9A:01:EC:59:17:D7:C0:43:74:DA: |
| (0) | 90:B0:43:8D:20:1A:E7:D3:58:6A:7F:BE:61:A9:B9:3B: |
| (0) | 94:BA:DF:B3:02:21:00:AA:34:CC:EB:BC:BE:CF:4E:E1: |
| (0) | 01:32:FB:36:9F:61:64:0E:78:B8:21:21:7C:0C:EE:38: |
| (0) | CA:AF:00:C6:21:26:FB |
| (0) | Signed Certificate Timestamp: |
| (0) | Version : v1 (0x0) |
| (0) | Log ID : E8:3E:D0:DA:3E:F5:06:35:32:E7:57:28:BC:89:6B:C9: |
| (0) | 03:D3:CB:D1:11:6B:EC:EB:69:E1:77:7D:6D:06:BD:6E |
| (0) | Timestamp : May 15 20:29:39.629 2023 GMT |
| (0) | Extensions: none |
| (0) | Signature : ecdsa-with-SHA256 |
| (0) | 30:45:02:21:00:DF:50:81:31:A3:FD:12:52:78:1B:24: |
| (0) | F9:4D:4D:34:42:F3:EC:E5:A4:50:71:B9:70:64:9D:74: |
| (0) | 35:B0:4A:37:CD:02:20:22:F5:FC:F9:02:00:D4:EE:3E: |
| (0) | 5E:02:04:11:7B:66:52:B2:20:BF:61:FC:F1:6C:11:D5: |
| (0) | 8B:21:EB:32:F4:26:0D |
| (0) | Signature (256 octets) |
| (0) | ab:8d:9b:c4:5f:3c:24:56:b4:00:95:c4:1e:bc:51:cd |
| (0) | 76:61:88:bb:d6:5b:44:1d:24:74:cd:20:35:ca:de:89 |
| (0) | f0:e3:32:65:10:fc:bf:8f:bc:8b:d9:14:a0:16:44:bd |
| (0) | ee:7d:71:84:d5:49:e7:d7:f5:bb:fb:13:94:c7:3e:d0 |
| (0) | c7:b0:3f:41:f3:f8:9f:7c:6e:e0:5a:83:8a:cb:27:67 |
| (0) | 13:cd:ab:0c:50:0d:1c:a6:57:53:c3:1a:b7:13:8d:ca |
| (0) | 2c:0d:c3:4d:fb:15:ba:22:65:5e:4c:2b:c8:e8:fd:4d |
| (0) | 86:03:99:bc:d9:9a:5e:4f:26:30:d0:ab:e5:14:ca:25 |

| | |
|------------------------------------|---|
| (0) | 08:5f:78:3f:cf:9a:b1:12:50:d9:c6:f4:cb:5a:8e:19 |
| (0) | aa:48:34:85:7c:e5:b4:0c:19:82:75:b2:e5:45:28:3f |
| (0) | e0:d7:5a:8b:ce:31:7e:d7:8a:58:88:d8:41:1f:24:36 |
| (0) | 20:6a:e9:21:29:49:fa:35:70:7d:4c:9a:ef:65:9c:66 |
| (0) | 99:57:93:09:61:5c:09:c9:3d:cf:4a:69:f8:4b:8d:e8 |
| (0) | 06:d9:f2:cd:25:50:ed:75:8f:23:86:90:48:fb:e8:7f |
| (0) | 8f:05:40:fa:ea:d7:37:c1:80:bb:46:a1:c0:ed:a9:d4 |
| (0) | 98:ec:29:68:c7:86:4a:d0:2a:a4:fe:f0:6c:a0:dd:ae |
| (1)CERTIFICATE 1 | |
| (1)Version | 3 (0x2) |
| (1)Serial Number | 91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a |
| (1)Signature Algorithm | sha256WithRSAEncryption |
| (1)ISSUER NAME | |
| countryName | US |
| organizationName | Internet Security Research Group |
| commonName | ISRG Root X1 |
| (1)SUBJECT NAME | |
| countryName | US |
| organizationName | Let's Encrypt |
| commonName | R3 |
| (1)Valid From | Sep 4 00:00:00 2020 GMT |
| (1)Valid Till | Sep 15 16:00:00 2025 GMT |
| (1)Public Key Algorithm | rsaEncryption |
| (1)RSA Public Key | (2048 bit) |
| (1) | RSA Public-Key: (2048 bit) |
| (1) | Modulus: |
| (1) | 00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55: |
| (1) | 92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5: |
| (1) | 2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47: |
| (1) | 94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42: |
| (1) | a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38: |
| (1) | e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa: |
| (1) | 37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52: |
| (1) | 45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de: |
| (1) | 60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b: |
| (1) | d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8: |
| (1) | 30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17: |
| (1) | c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46: |
| (1) | e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7: |
| (1) | a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98: |
| (1) | 09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af: |
| (1) | 63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d: |
| (1) | a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b: |
| (1) | db:15 |
| (1) | Exponent: 65537 (0x10001) |
| (1)X509v3 EXTENSIONS | |
| (1)X509v3 Key Usage | critical |
| (1) | Digital Signature, Certificate Sign, CRL Sign |
| (1)X509v3 Extended Key Usage | TLS Web Client Authentication, TLS Web Server Authentication |
| (1)X509v3 Basic Constraints | critical |
| (1) | CA:TRUE, pathlen:0 |
| (1)X509v3 Subject Key Identifier | 14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 |
| (1)X509v3 Authority Key Identifier | keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E |
| (1)Authority Information Access | CA Issuers - URI:http://x1.i.lencr.org/ |
| (1)X509v3 CRL Distribution Points | |

| | |
|--------------------------------|---|
| (1) | Full Name: |
| (1) | URI:http://x1.c.lencr.org/ |
| (1)X509v3 Certificate Policies | Policy: 2.23.140.1.2.1 |
| (1) | Policy: 1.3.6.1.4.1.44947.1.1.1 |
| (1)Signature | (512 octets) |
| (1) | 85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98 |
| (1) | 63:ad:75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3 |
| (1) | ed:f8:20:bf:5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de |
| (1) | e4:20:9f:a6:ef:8b:b2:03:e7:a2:b5:16:3c:91:ce:b4 |
| (1) | ed:39:02:e7:7c:25:8a:47:e6:65:6e:3f:46:f4:d9:f0 |
| (1) | ce:94:2b:ee:54:ce:12:bc:8c:27:4b:b8:c1:98:2f:a2 |
| (1) | af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:2d:08:f9:08 |
| (1) | 57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:2a:c8 |
| (1) | 9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c |
| (1) | 5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed |
| (1) | 63:b9:21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22 |
| (1) | ae:10:0d:43:97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1 |
| (1) | bd:30:bf:87:6e:2b:2a:ff:21:4e:1b:05:c3:f5:18:97 |
| (1) | f0:5e:ac:c3:a5:b8:6a:f0:2e:bc:3b:33:b9:ee:4b:de |
| (1) | cc:fc:e4:af:84:0b:86:3f:c0:55:43:36:f6:68:e1:36 |
| (1) | 17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:d0:63:39:35 |
| (1) | 39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:ce:0c |
| (1) | 02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53 |
| (1) | f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4 |
| (1) | 29:0e:f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18 |
| (1) | a1:79:bb:e7:5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61 |
| (1) | 71:25:2a:af:df:ed:25:50:52:68:8b:92:dc:e5:d6:b5 |
| (1) | e3:da:7d:d0:87:6c:84:21:31:ae:82:f5:fb:b9:ab:c8 |
| (1) | 89:17:3d:e1:4c:e5:38:0e:f6:bd:2b:bd:96:81:14:eb |
| (1) | d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:5b:b8:48:cd |
| (1) | fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:ea:7c |
| (1) | 93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff |
| (1) | 28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f |
| (1) | 0b:d2:52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85 |
| (1) | 5d:7e:5d:66:29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42 |
| (1) | cd:c4:4e:c6:25:38:44:50:6d:ec:ce:00:55:18:fe:e9 |
| (1) | 49:64:d4:4e:ca:97:9c:b4:5b:c0:73:a8:ab:b8:47:c2 |
| (2)CERTIFICATE 2 | |
| (2)Version | 3 (0x2) |
| (2)Serial Number | 40:01:77:21:37:d4:e9:42:b8:ee:76:aa:3c:64:0a:b7 |
| (2)Signature Algorithm | sha256WithRSAEncryption |
| (2)ISSUER NAME | |
| organizationName | Digital Signature Trust Co. |
| commonName | DST Root CA X3 |
| (2)SUBJECT NAME | |
| countryName | US |
| organizationName | Internet Security Research Group |
| commonName | ISRG Root X1 |
| (2)Valid From | Jan 20 19:14:03 2021 GMT |
| (2)Valid Till | Sep 30 18:14:03 2024 GMT |
| (2)Public Key Algorithm | rsaEncryption |
| (2)RSA Public Key | (4096 bit) |
| (2) | RSA Public-Key: (4096 bit) |
| (2) | Modulus: |
| (2) | 00:ad:e8:24:73:f4:14:37:f3:9b:9e:2b:57:28:1c: |

| | |
|------------------------------------|---|
| (2) | 87:be:dc:b7:df:38:90:8c:6e:3c:e6:57:a0:78:f7: |
| (2) | 75:c2:a2:fe:f5:6a:6e:f6:00:4f:28:db:de:68:86: |
| (2) | 6c:44:93:b6:b1:63:fd:14:12:6b:bf:1f:d2:ea:31: |
| (2) | 9b:21:7e:d1:33:3c:ba:48:f5:dd:79:df:b3:b8:ff: |
| (2) | 12:f1:21:9a:4b:c1:8a:86:71:69:4a:66:66:6c:8f: |
| (2) | 7e:3c:70:bf:ad:29:22:06:f3:e4:c0:e6:80:ae:e2: |
| (2) | 4b:8f:b7:99:7e:94:03:9f:d3:47:97:7c:99:48:23: |
| (2) | 53:e8:38:ae:4f:0a:6f:83:2e:d1:49:57:8c:80:74: |
| (2) | b6:da:2f:d0:38:8d:7b:03:70:21:1b:75:f2:30:3c: |
| (2) | fa:8f:ae:dd:da:63:ab:eb:16:4f:c2:8e:11:4b:7e: |
| (2) | cf:0b:e8:ff:b5:77:2e:f4:b2:7b:4a:e0:4c:12:25: |
| (2) | 0c:70:8d:03:29:a0:e1:53:24:ec:13:d9:ee:19:bf: |
| (2) | 10:b3:4a:8c:3f:89:a3:61:51:de:ac:87:07:94:f4: |
| (2) | 63:71:ec:2e:e2:6f:5b:98:81:e1:89:5c:34:79:6c: |
| (2) | 76:ef:3b:90:62:79:e6:db:a4:9a:2f:26:c5:d0:10: |
| (2) | e1:0e:de:d9:10:8e:16:fb:b7:f7:a8:f7:c7:e5:02: |
| (2) | 07:98:8f:36:08:95:e7:e2:37:96:0d:36:75:9e:fb: |
| (2) | 0e:72:b1:1d:9b:bc:03:f9:49:05:d8:81:dd:05:b4: |
| (2) | 2a:d6:41:e9:ac:01:76:95:0a:0f:d8:df:d5:bd:12: |
| (2) | 1f:35:2f:28:17:6c:d2:98:c1:a8:09:64:77:6e:47: |
| (2) | 37:ba:ce:ac:59:5e:68:9d:7f:72:d6:89:c5:06:41: |
| (2) | 29:3e:59:3e:dd:26:f5:24:c9:11:a7:5a:a3:4c:40: |
| (2) | 1f:46:a1:99:b5:a7:3a:51:6e:86:3b:9e:7d:72:a7: |
| (2) | 12:05:78:59:ed:3e:51:78:15:0b:03:8f:8d:d0:2f: |
| (2) | 05:b2:3e:7b:4a:1c:4b:73:05:12:fc:c6:ea:e0:50: |
| (2) | 13:7c:43:93:74:b3:ca:74:e7:8e:1f:01:08:d0:30: |
| (2) | d4:5b:71:36:b4:07:ba:c1:30:30:5c:48:b7:82:3b: |
| (2) | 98:a6:7d:60:8a:a2:a3:29:82:cc:ba:bd:83:04:1b: |
| (2) | a2:83:03:41:a1:d6:05:f1:1b:c2:b6:f0:a8:7c:86: |
| (2) | 3b:46:a8:48:2a:88:dc:76:9a:76:bf:1f:6a:a5:3d: |
| (2) | 19:8f:eb:38:f3:64:de:c8:2b:0d:0a:28:ff:f7:db: |
| (2) | e2:15:42:d4:22:d0:27:5d:e1:79:fe:18:e7:70:88: |
| (2) | ad:4e:e6:d9:8b:3a:c6:dd:27:51:6e:ff:bc:64:f5: |
| (2) | 33:43:4f |
| (2) | Exponent: 65537 (0x10001) |
| (2)X509v3 EXTENSIONS | |
| (2)X509v3 Basic Constraints | critical |
| (2) | CA:TRUE |
| (2)X509v3 Key Usage | critical |
| (2) | Certificate Sign, CRL Sign |
| (2)Authority Information Access | CA Issuers - URI:http://apps.identrust.com/roots/dstrootca3.p7c |
| (2)X509v3 Authority Key Identifier | keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:10 |
| (2)X509v3 Certificate Policies | Policy: 2.23.140.1.2.1 |
| (2) | Policy: 1.3.6.1.4.1.44947.1.1.1 |
| (2) | CPS: http://cps.root-x1.letsencrypt.org |
| (2)X509v3 CRL Distribution Points | |
| (2) | Full Name: |
| (2) | URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl |
| (2)X509v3 Subject Key Identifier | 79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E |
| (2)Signature | (256 octets) |
| (2) | 0a:73:00:6c:96:6e:ff:0e:52:d0:ae:dd:8c:e7:5a:06 |
| (2) | ad:2f:a8:e3:8f:bf:c9:0a:03:15:50:c2:e5:6c:42:bb |
| (2) | 6f:9b:f4:b4:4f:c2:44:88:08:75:cc:eb:07:9b:14:62 |
| (2) | 6e:78:de:ec:27:ba:39:5c:f5:a2:a1:6e:56:94:70:10 |
| (2) | 53:b1:bb:e4:af:d0:a2:c3:2b:01:d4:96:f4:c5:20:35 |

| | |
|-----|---|
| (2) | 33:f9:d8:61:36:e0:71:8d:b4:b8:b5:aa:82:45:95:c0 |
| (2) | f2:a9:23:28:e7:d6:a1:cb:67:08:da:a0:43:2c:aa:1b |
| (2) | 93:1f:c9:de:f5:ab:69:5d:13:f5:5b:86:58:22:ca:4d |
| (2) | 55:e4:70:67:6d:c2:57:c5:46:39:41:cf:8a:58:83:58 |
| (2) | 6d:99:fe:57:e8:36:0e:f0:0e:23:aa:fd:88:97:d0:e3 |
| (2) | 5c:0e:94:49:b5:b5:17:35:d2:2e:bf:4e:85:ef:18:e0 |
| (2) | 85:92:eb:06:3b:6c:29:23:09:60:dc:45:02:4c:12:18 |
| (2) | 3b:e9:fb:0e:de:dc:44:f8:58:98:ae:ea:bd:45:45:a1 |
| (2) | 88:5d:66:ca:fe:10:e9:6f:82:c8:11:42:0d:fb:e9:ec |
| (2) | e3:86:00:de:9d:10:e3:38:fa:a4:7d:b1:d8:e8:49:82 |
| (2) | 84:06:9b:2b:e8:6b:4f:01:0c:38:77:2e:f9:dd:e7:39 |


Web Server Supports HTTP Request Pipelining

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
 QID: 86565
 Category: Web server
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 02/23/2005

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker, it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

RESULT:

GET / HTTP/1.1
 Host:3.29.26.82:443

GET /Q_Evasive/ HTTP/1.1
 Host:3.29.26.82:443


Default Web Page

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 12230
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 03/16/2019

THREAT:

The Result section displays the default Web page for the Web server.

RESULT:

GET / HTTP/1.0

Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

```
{\"type\": \"collection\", \"links\": {\"self\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/\", \"actions\": {}, \"pagination\": {\"limit\": 1000, \"total\": 4}, \"sort\": {\"order\": \"asc\", \"reverse\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/?order=desc\"}, \"resourceType\": \"apiRoot\", \"data\": [{\"apiVersion\": {\"group\": \"meta.cattle.io\", \"path\": \"/meta\", \"version\": \"v1\"}, \"baseType\": \"apiRoot\", \"links\": {\"apiRoots\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/apiroots\", \"root\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta\", \"schemas\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/schemas\", \"self\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta\", \"subscribe\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/subscribe\"}, \"type\": \"apiRoot\"}], {\"group\": \"management.cattle.io\", \"path\": \"/v3\", \"version\": \"v3\"}, \"baseType\": \"apiRoot\", \"links\": {\"authConfigs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/authconfigs\", \"catalogs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/catalogs\", \"cloudCredentials\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cloudcredentials\", \"clusterAlertGroups\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteralertgroups\", \"clusterAlertRules\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteralerts\", \"clusterCatalogs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clustercatalogs\", \"clusterMonitorGraphs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clustermonitorgraphs\", \"clusterRegistrationTokens\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusterregistrationtokens\", \"clusterRoleTemplateBindings\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusterroletemplatebindings\", \"clusterTemplateRevisions\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteremplaterevisions\", \"clusterTemplates\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteremplates\", \"clusters\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusters\", \"composeConfigs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/composeconfigs\", \"dynamicSchemas\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/dynamicschemas\", \"etcdBackups\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/etcdbackups\", \"features\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/features\", \"fleetWorkspaces\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/fleetworkspaces\", \"globalDnsProviders\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globaldnsproviders\", \"globalDnses\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globaldnses\", \"globalRoleBindings\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globalrolebindings\", \"globalRoles\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globalroles\", \"groupMembers\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/groupmembers\", \"groups\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/groups\", \"kontainerDrivers\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/kontainerdrivers\", \"ldapConfigs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/ldapconfigs\", \"managementSecrets\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/managementsecrets\", \"monitorMetrics\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/monitormetrics\", \"multiClusterAppRevisions\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/multiclusterapprevisions\", \"multiClusterApps\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/multiclusterapps\", \"nodeDrivers\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodedrivers\", \"nodePools\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodepools\", \"nodeTemplates\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodetemplates\", \"nodes\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodes\", \"notifiers\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/notifiers\", \"podSecurityAdmissionConfigurationTemplates\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/podsecurityadmissionconfigurationtemplates\", \"podSecurityPolicyTemplateProjectBindings\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/podsecuritypolicytemplateprojectbindings\", \"podSecurityPolicyTemplates\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/podsecuritypolicytemplates\", \"preferences\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/preferences\", \"principals\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/principals\", \"projectAlertGroups\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectalertgroups\", \"projectAlertRules\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectalerts\", \"projectCatalogs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectcatalogs\", \"projectMonitorGraphs\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectmonitorgraphs\", \"projectNetworkPolicies\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectnetworkpolicies\", \"projectRoleTemplateBindings\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectroletemplatebindings\", \"projects\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projects\", \"rancherUserNotifications\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rancherusernotifications\", \"rkeAddons\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rkeaddons\", \"rkeK8sServiceOptions\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rkek8sserviceoptions\", \"rkeK8sSystemImages\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rkek8ssystemimages\", \"roleTemplates\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/roletemplates\", \"root\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3\", \"samlTokens\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/samltokens\", \"self\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3\", \"settings\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/settings\", \"subscribe\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/subscribe\", \"templateVersions\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/templates\", \"tokens\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/tokens\", \"users\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/users\"}], {\"apiVersion\": {\"group\": \"cluster.cattle.io\", \"path\": \"/v3/cluster\", \"version\": \"v3\"}, \"baseType\": \"apiRoot\", \"links\": {\"apiServices\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/apiservices\", \"namespaces\": \"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/namespaces\", \"persistentVolumes\": \"https://ec2-3-29-26-82.me-central-1
```

```
compute.amazonaws.com/v3/cluster/persistentvolumes", "root": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster", "self": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster", "storageClasses": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/storageclasses", "subscribe": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/subscribe"}, "type": "apiRoot"}, {"apiVersion": {"group": "project.cattle.io", "path": "/v3/project", "version": "v3"}, "baseType": "apiRoot", "links": {"alertmanagers": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/alertmanagers", "appRevisions": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/apprevisions", "apps": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/apps", "basicAuths": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/basicauths", "certificates": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/certificates", "configMaps": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/configmaps", "cronJobs": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/cronjobs", "daemonSets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/daemonsets", "deployments": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/deployments", "dnsRecords": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/dnsrecords", "dockerCredentials": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/dockercredentials", "horizontalPodAutoscalers": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/horizontalpodautoscalers", "ingresses": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/ingresses", "jobs": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/jobs", "namespacedBasicAuths": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedbasicauths", "namespacedCertificates": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedcertificates", "namespacedDockerCredentials": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespaceddockercredentials", "namespacedSecrets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedsecrets", "namespacedServiceAccountTokens": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedserviceaccounttokens", "namespacedSshAuths": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedsshauths", "persistentVolumeClaims": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/persistentvolumeclaims", "pods": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/pods", "prometheusRules": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/prometheusrules", "prometheuses": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/prometheuses", "replicaSets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/replicasets", "replicationControllers": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/replicationcontrollers", "root": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project", "secrets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/secrets", "self": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project", "serviceAccountTokens": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/serviceaccounttokens", "serviceMonitors": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/servicemonitors", "services": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/services", "sshAuths": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/sshauths", "statefulSets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/statefulsets", "subscribe": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/subscribe", "workloads": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/workloads"}, "type": "apiRoot"}]}
```


Default Web Page (Follow HTTP Redirection)

port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 13910
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/05/2020

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

SOLUTION:

Patch:

Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (<https://www.qnap.com/en/security-advisory/nas-201911-01>)

RESULT:

GET / HTTP/1.0
Host: ec2-3-29-26-82.me-central-1.compute.amazonaws.com

```
{"type": "collection", "links": {"self": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/subscribe", "type": "apiRoot"}}
```

com/","actions":{},"pagination":{"limit":1000,"total":4},"sort":{"order":"asc","reverse":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/?order=desc"},"resourceType":"apiRoot","data":{"apiVersion":{"group":"meta.cattle.io","path":"/meta","version":"v1"},"baseType":"apiRoot","links":{"apiRoots":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/apiroots","root":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta","schemas":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/schemas","self":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta","subscribe":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/meta/subscribe"},"type":"apiRoot"},"apiVersion":{"group":"management.cattle.io","path":"/v3","version":"v3"},"baseType":"apiRoot","links":{"authConfigs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/authconfigs","catalogs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/catalogs","cloudCredentials":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cloudcredentials","clusterAlertGroups":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteralertgroups","clusterAlertRules":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteralertrules","clusterAlerts":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteralerts","clusterCatalogs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clustercatalogs","clusterMonitorGraphs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clustermonitorgraphs","clusterRegistrationTokens":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusterregistrationtokens","clusterRoleTemplateBindings":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusterroletemplatebindings"},"clusterTemplateRevisions":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteremplaterevisions","clusterTemplates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusteremplates","clusters":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/clusters","composeConfigs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/composeconfigs","dynamicSchemas":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/dynamicschemas","etcdBackups":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/etcdbackups","features":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/features","fleetWorkspaces":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/fleetworkspaces","globalDnsProviders":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globaldnsproviders","globalDnses":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globaldnses","globalRoleBindings":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globalrolebindings","globalRoles":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/globalroles","groupMembers":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/groupmembers","groups":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/groups","kontainerDrivers":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/kontainerdrivers","ldapConfigs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/ldapconfigs","managementSecrets":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/managementsecrets","monitorMetrics":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/monitormetrics","multiClusterAppRevisions":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/multiclusterapprevisions","multiClusterApps":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/multiclusterapps","nodeDrivers":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodedrivers","nodePools":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodepools","nodeTemplates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodetemplates","nodes":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/nodes","notifiers":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/notifiers","podSecurityAdmissionConfigurationTemplates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/podsecurityadmissionconfigurationtemplates","podSecurityPolicyTemplateProjectBindings":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/podsecuritypolicytemplateprojectbindings","podSecurityPolicyTemplates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/podsecuritypolicytemplates","preferences":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/preferences","principals":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/principals","projectAlertGroups":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectalertgroups","projectAlertRules":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectalertrules","projectAlerts":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectalerts","projectCatalogs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectcatalogs","projectMonitorGraphs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectmonitorgraphs","projectNetworkPolicies":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectnetworkpolicies","projectRoleTemplateBindings":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projectroletemplatebindings","projects":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/projects","rancherUserNotifications":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rancherusernotifications","rkeAddons":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rkeaddons","rkeK8sServiceOptions":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rkek8sserviceoptions","rkeK8sSystemImages":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/rkek8ssystemimages","roleTemplates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/roletemplates","root":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3","samlTokens":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/samltokens","self":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3","settings":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/settings","subscribe":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/subscribe","templateVersions":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/templates","tokens":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/tokens","users":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/users"},"type":"apiRoot"},"apiVersion":{"group":"cluster.cattle.io","path":"/v3/cluster","version":"v3"},"baseType":"apiRoot","links":{"apiServices":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/apiservices","namespaces":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/namespaces","persistentVolumes":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/persistentvolumes","root":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster","self":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster","storageClasses":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/storageclasses","subscribe":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/cluster/subscribe"},"type":"apiRoot"},"apiVersion":{"group":"project.cattle.io","path":"/v3/project","version":"v3"},"baseType":"apiRoot","links":{"alertmanagers":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/alertmanagers","appRevisions":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/apprevisions","apps":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/apps","basicAuths":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/basicauths","certificates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/certificates","configMaps":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/configmaps","cronJobs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/cronjobs","daemonSets":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/daemonsets","deployments":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/deployments","dnsRecords":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/dnsrecords","dockerCredentials":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/dockercredentials","horizontalPodAutoscalers":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/horizontalpodautoscalers","ingresses":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/ingresses","jobs":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/jobs","namespacedBasicAuths":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedbasicauths","namespacedCertificates":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedcertificates","namespacedDockerCredentials":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespaceddockercredentials","namespacedSecrets":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedsecrets","namespacedServiceAccountTokens":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedserviceaccounttokens","namespacedSshAuths":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/namespacedsshauths","persistentVolumeClaims":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/persistentvolumeclaims","pods":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/pods","prometheusRules":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/prometheusrules","prometheuses":"https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/prometheuses","replicaSets":"https://ec2-3-29-26-82.me-

```
central-1.compute.amazonaws.com/v3/project/replicasets", "replicationControllers": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/replicationcontrollers", "root": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project", "secrets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/secrets", "self": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project", "serviceAccountTokens": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/serviceaccounttokens", "serviceMonitors": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/serviceaccounttokens", "services": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/services", "sshAuths": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/sshauths", "statefulSets": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/statefulsets", "subscribe": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/subscribe", "workloads": "https://ec2-3-29-26-82.me-central-1.compute.amazonaws.com/v3/project/workloads"}, "type": "apiRoot"}}}
```

Appendices

Hosts Scanned

3.29.26.82

Hosts Not Alive

3.29.30.141

Option Profile

Scan

| | |
|---|---------------|
| Scanned TCP Ports: | Full |
| Scanned UDP Ports: | Standard Scan |
| Scan Dead Hosts: | Off |
| Load Balancer Detection: | Off |
| Password Brute Forcing: | Standard |
| Vulnerability Detection: | Complete |
| Windows Authentication: | Disabled |
| SSH Authentication: | Disabled |
| Oracle Authentication: | Disabled |
| SNMP Authentication: | Disabled |
| Perform 3-way Handshake: | Off |
| Overall Performance: | Custom |
| Hosts to Scan in Parallel-External Scanner: | 15 |
| Hosts to Scan in Parallel-Scanner Appliances: | 15 |
| Processes to Run in Parallel-Total: | 10 |
| Processes to Run in Parallel-HTTP: | 10 |
| Packet (Burst) Delay: | Medium |

Advanced

| | |
|---|---|
| Hosts Discovery: | TCP Standard Scan, UDP Standard Scan, ICMP On |
| Ignore RST packets: | Off |
| Ignore firewall-generated SYN-ACK packets: | Off |
| Do not send ACK or SYN-ACK packets during host discovery: | Off |

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.






A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS




compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels





A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.


| Severity | Level | Description |
|---|----------|---|
|  1 | Minimal | Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. |
|  2 | Medium | Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. |
|  3 | Serious | Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. |
|  4 | Critical | Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. |
|  5 | Urgent | Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. |

| Severity | Level | Description |
|--|--------|---|
|  Low | Low | A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance. |
|  Medium | Medium | A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance. |
|  High | High | A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance. |


Potential Vulnerability Levels


A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.


| Severity | Level | Description |
|---|----------|--|
|  1 | Minimal | If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. |
|  2 | Medium | If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. |
|  3 | Serious | If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. |
|  4 | Critical | If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. |

 5 Urgent If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

| Severity | Level | Description |
|----------|-------|-------------|
|----------|-------|-------------|

| | | |
|---|-----|---|
|  | Low | A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance. |
|---|-----|---|


| | | |
|---|--------|--|
|  | Medium | A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance. |
|---|--------|--|


| | | |
|---|------|---|
|  | High | A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance. |
|---|------|---|

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

| Severity | Level | Description |
|----------|-------|-------------|
|----------|-------|-------------|

| | | |
|---|-----------|---|
|  | 1 Minimal | Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls. |
|---|-----------|---|

| | | |
|---|----------|--|
|  | 2 Medium | Intruders may be able to determine the operating system running on the host, and view banner versions. |
|---|----------|--|

| | | |
|---|-----------|--|
|  | 3 Serious | Intruders may be able to detect highly sensitive data, such as global system user lists. |
|---|-----------|--|