







Top 25 Remediations by Risk

June 6, 2022 5:09:44 PM CLT

AMER_CHILE_TOP25



Remediation	Assets	Vulnerabilities			Risk 
1. 2022-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5013942)	14	1,561	10	0	304,487
2. 2022-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5013941)	3	1,065	12	1	241,264
3. 2022-05 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB5013945)	5	1,102	13	0	237,226
4. Upgrade to the latest version of PHP	3	309	15	0	160,286
5. Upgrade to the latest version of Mozilla Firefox	11	776	2	0	150,617
6. Upgrade to the latest version of Oracle Java	7	343	3	0	111,737
7. Disable insecure TLS/SSL protocol support	79	210	38	0	106,906
8. Protect the unquoted search paths or elements in the registry	137	137	0	0	101,618
9. Upgrade VMware ESXi to the latest version	4	252	8	0	92,763
10. Upgrade the CIFS authentication method	111	111	0	0	82,397
11. Secure the SNMP installation	42	91	0	0	75,533
12. 2022-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5013952)	5	394	2	0	73,390
13. Update McAfee Agent to version 5.7.6	157	314	0	0	59,155
14. Secure the FTP account	12	82	0	0	57,268
15. Obtain a new certificate from your CA and ensure the server configuration is correct	77	77	0	0	53,712
16. Fix the subject's Common Name (CN) field in the certificate	63	63	0	0	52,438
17. Upgrade to the latest version of Google Chrome	14	463	0	0	52,144
18. 2022-04 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB5012649)	6	252	6	0	49,644

Remediation	Assets	Vulnerabilities			Risk 
19. Configure SMB signing for Windows	46	58	0	0	49,264
20. Disable HTTP OPTIONS method	73	73	0	0	42,297
21. Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled	76	76	0	0	41,630
22. Disable TLS/SSL support for static key cipher suites	87	87	0	0	41,401
23. Upgrade to the latest version of Microsoft Edge	17	360	0	0	41,038
24. 2022-05 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5013942)	4	232	0	0	40,513
25. Upgrade to the latest version of OpenSSL	6	99	10	0	37,449

1. 2022-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5013942)

Remediation Steps

Download and apply the patch from: <https://support.microsoft.com/kb/5013942> <https://support.microsoft.com/kb/5013942>

Assets

Name	IP Address	Site
CLODIL0110.ad.global	192.168.0.12	AD_AMER,Rapid7 Insight Agents
CLODIL0126.ad.global	192.168.1.141	Rapid7 Insight Agents
CLODIL0127.ad.global	192.168.0.14	Rapid7 Insight Agents
CLODIL0130.ad.global	192.168.0.5	Rapid7 Insight Agents
CLODIL0131.ad.global	192.168.100.11	Rapid7 Insight Agents,AD_AMER
CLODIL0132.ad.global	192.168.8.102	Rapid7 Insight Agents
CLODIL0133.ad.global	192.168.140.102	Rapid7 Insight Agents
CLODIL0134.ad.global	192.168.0.9	Rapid7 Insight Agents
CLODIL0136.ad.global	192.168.1.8	Rapid7 Insight Agents
CLODIL0140.ad.global	10.244.231.67	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLODIL0141.ad.global	10.244.231.109	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AD_AMER
CLSAND0020.ad.global	10.244.231.48	AMER GLOBAL - UTC -6,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_A
CLSANL0087.ad.global	192.168.1.81	Rapid7 Insight Agents
CLSANL0088.ad.global	192.168.0.7	Rapid7 Insight Agents

2. 2022-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5013941)

Remediation Steps

Download and apply the patch from: <https://support.microsoft.com/kb/5013941> <https://support.microsoft.com/kb/5013941>

Assets

Name	IP Address	Site
CLSANAPPTTEST01	10.208.32.5	TI_Cloud, TI_Log4Shell_all_internall
CLSANDBTEST01	10.208.32.6	TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, TI_Cloud
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA, TI_all_AD_Divisional_Servers, AD_AMER, TI_Log4Shell_all_internall, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_all_servers

3. 2022-05 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB5013945)

Remediation Steps

Download and apply the patch from: <https://support.microsoft.com/kb/5013945> <https://support.microsoft.com/kb/5013945>

Assets

Name	IP Address	Site
CLODIL0054.ad.global	10.244.231.106	Rapid7 Insight Agents
CLODIL0077.ad.global	192.168.240.131	TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents,AD_AMER
CLODIL0078.ad.global	192.168.1.90	Rapid7 Insight Agents
CLODIL0084	10.244.230.37	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0086.ad.global	10.244.230.52	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents

4. Upgrade to the latest version of PHP

Remediation Steps

Download and apply the upgrade from: <http://www.php.net/downloads.php>

The latest version of PHP is 8.1.3
<http://www.php.net/downloads.php>

Assets

Name	IP Address	Site
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC, AD_AMER, AMER GLOBAL - BRASIL/CHILE
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_EMEIA, TI_Log4Shell_all_servers, TI_all_AD_Divisional_Servers, AMER GLOBAL - UTC -6, AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC, TI_all_AD_Divisional_Servers, AMER GLOBAL - BRASIL/CHILE, AD_AMER, TI_Log4Shell_all_internall

5. Upgrade to the latest version of Mozilla Firefox

Remediation Steps

Install the latest version of Mozilla Firefox from the [Mozilla Products](#) page.

Assets

Name	IP Address	Site
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0026.ad.global	192.168.0.6	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0048.ad.global	192.168.1.9	AD_AMER,Rapid7 Insight Agents
CLODIL0086.ad.global	10.244.230.52	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0138.ad.global	192.168.100.20	Rapid7 Insight Agents,AD_AMER
CLSANL0035.ad.global	192.168.1.16	AD_AMER,Rapid7 Insight Agents
CLSANL0040.ad.global	192.168.4.52	Rapid7 Insight Agents,AD_AMER
CLSANL0047.ad.global	192.168.1.85	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANL0059.ad.global	192.168.1.81	AD_AMER,Rapid7 Insight Agents
CLSANL0062.ad.global	192.168.100.5	Rapid7 Insight Agents,AD_AMER
clodid0007.ad.global	10.244.231.52	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE

6. Upgrade to the latest version of Oracle Java

Remediation Steps

Download and apply the upgrade from: <https://www.java.com/en/download/manual.jsp>
<https://www.java.com/en/download/manual.jsp>

Assets

Name	IP Address	Site
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0040.ad.global	192.168.0.108	AD_AMER,Rapid7 Insight Agents
CLSANL0040.ad.global	192.168.4.52	Rapid7 Insight Agents,AD_AMER
CLSANL0058.ad.global	192.168.0.131	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsans-dcfacele.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC

7. Disable insecure TLS/SSL protocol support

Remediation Steps

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

Assets

Name	IP Address	Site
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLODISDC0001.ad.global	10.244.229.240	AD_Domain_controllers,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
CLSANAPPTTEST01	10.208.32.5	TI_Cloud,TI_Log4Shell_all_internall
CLSANDBTEST01	10.208.32.6	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Cloud
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
EPSON2578E2	10.34.45.52	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.133.251.1	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.229.2	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - UTC -6
Unknown	10.244.230.1	AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.244.230.153	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
Unknown	10.244.230.49	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA

Name	IP Address	Site
Unknown	10.244.230.49	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC-6,TI_Log4Shell_all_internall
Unknown	10.244.230.98	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.107	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.118	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.12	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.120	AD_AMER,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.122	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.131	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.136	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.141	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.142	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.143	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.145	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.146	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.17	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.19	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.2	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_All_Linux,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.22	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.24	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.29	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.3	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_All_Linux
Unknown	10.244.231.31	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.1	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.162	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.3	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.31	TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.32	TI_All_Linux,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.33	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_All_Linux
Unknown	10.34.45.34	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_All_Linux,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.35	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.4	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
Unknown	10.34.45.6	TI_Log4Shell_all_internall, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.7	TI_Log4Shell_all_internall, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.9	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_EMEIA
Unknown	200.111.184.180	AMER GLOBAL-External, TI_Log4Shell_external
Unknown	200.111.184.183	AMER GLOBAL-External, TI_Log4Shell_external
bdc-bui-04.ad.global	10.244.229.3	TI_Log4Shell_all_servers, AD_AMER, TI_all_AD_Divisional_Servers, AMER GLOBAL - UTC - 6, TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers, AMER GLOBAL - UTC - 6, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC, AD_AMER, TI_Log4Shell_all_servers, TI_Log4Shell_all_internall
clodid0007.ad.global	10.244.231.52	AD_AMER, TI_Log4Shell_all_internall, AMER GLOBAL - BRASIL/CHILE
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_servers, AD_AMER, AMER GLOBAL - UTC - 6, TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AD_AMER, TI_all_AD_Divisional_Servers, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA, AD_AMER, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, AMER GLOBAL - BRASIL/CHILE, TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, AD_AMER, TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_internall, TI_all_AD_Divisional_Servers, TI_Log4Shell_EMEIA, AD_AMER, AMER GLOBAL - UTC - 6, TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall, AD_AMER, TI_all_AD_Divisional_Servers, AMER GLOBAL - UTC - 6, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers, AD_AMER, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - UTC - 6, TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_servers, AMER GLOBAL - UTC - 6, AD_AMER, TI_Log4Shell_HID_AMER_APAC, TI_all_AD_Divisional_Servers, TI_Log4Shell_EMEIA, TI_Log4Shell_all_internall
clsans-dcfacale.ad.global	10.244.229.26	TI_Log4Shell_EMEIA, TI_Log4Shell_all_internall, AD_AMER, AMER GLOBAL - UTC - 6, TI_all_AD_Divisional_Servers, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0002.ad.global	10.244.229.100	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_
clsansis0001.ad.global	10.244.229.11	AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers
clsanst0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers
np2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall

8. Protect the unquoted search paths or elements in the registry

Remediation Steps

There exist 3 potential workarounds:

- Modify the specified registry value(s) so that they are properly surrounded with quotation marks.
- Apply file system ACLs that ensure that only trusted users are able to write to the affected path(s). Note that this solution may not necessarily remedy this vulnerability depending on the security capabilities of the asset in question and how these capabilities are utilized.
- It is possible that the latest version of the affected software has patched this vulnerability, so try upgrading.

Assets

Name	IP Address	Site
CLODID0015.ad.global	10.34.45.154	TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC - 6,2020.12-Fireeye-NSA,AD_AMER,Rapid7 Insight Agents
CLODID0020.ad.global	10.34.45.140	TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_EMEIA,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODID0033.ad.global	10.244.230.21	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODID0037.ad.global	192.168.1.86	AD_AMER,Rapid7 Insight Agents
CLODID0043.ad.global	10.244.231.195	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,Rapid7 Insight Agents
CLODID0045.ad.global	10.244.231.14	AD_AMER,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC - 7,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,Rapid7 Insight Agents
CLODID0048.ad.global	10.244.231.66	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODID0049.ad.global	10.244.231.166	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AD_AMER,Rapid7 Insight Agents
CLODID0050.ad.global	10.34.45.122	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents,AD_AMER
CLODIL0001.ad.global	10.0.1.12	Rapid7 Insight Agents,AD_AMER
CLODIL0005.ad.global	192.168.0.7	Rapid7 Insight Agents,AD_AMER
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0014.ad.global	10.244.231.52	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0021.ad.global	192.168.1.20	AD_AMER,Rapid7 Insight Agents
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0026.ad.global	192.168.0.6	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0027.ad.global	10.244.231.146	TI_Log4Shell_all_internall,AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0028.ad.global	192.168.1.122	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0036.ad.global	10.244.231.42	AD_AMER,2021.02 - NSA-Fireeye,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6
CLODIL0038.ad.global	10.244.231.94	AD_AMER,2020.12-Fireeye-NSA,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
CLODIL0040.ad.global	192.168.0.108	AD_AMER,Rapid7 Insight Agents

Name	IP Address	Site
CLODIL0044.ad.global	10.244.230.63	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0045.ad.global	192.168.1.118	Rapid7 Insight Agents,AD_AMER
CLODIL0048.ad.global	192.168.1.9	AD_AMER,Rapid7 Insight Agents
CLODIL0049.ad.global	192.168.0.110	Rapid7 Insight Agents,AD_AMER
CLODIL0054.ad.global	10.244.231.106	Rapid7 Insight Agents
CLODIL0056.ad.global	10.244.231.174	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0057.ad.global	192.168.70.12	AD_AMER,Rapid7 Insight Agents
CLODIL0058.ad.global	10.244.231.45	Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0059.ad.global	192.168.8.100	Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_EMEIA
CLODIL0063.ad.global	10.34.45.108	Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0064.ad.global	192.168.1.3	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC
CLODIL0065.ad.global	10.34.45.125	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0067.ad.global	192.168.45.93	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0072.ad.global	192.168.43.132	AD_AMER,Rapid7 Insight Agents
CLODIL0073.ad.global	192.168.56.162	Rapid7 Insight Agents
CLODIL0076.ad.global	192.168.1.156	Rapid7 Insight Agents,AD_AMER
CLODIL0082.ad.global	10.244.230.44	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0083.ad.global	10.34.45.105	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0084	10.244.230.37	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0087.ad.global	192.168.1.126	AD_AMER,Rapid7 Insight Agents
CLODIL0088.ad.global	10.244.231.81	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0092.ad.global	192.168.1.88	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0093.ad.global	192.168.0.4	AD_AMER,Rapid7 Insight Agents
CLODIL0095.ad.global	10.244.231.91	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0096.ad.global	10.244.231.162	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0097.ad.global	10.34.45.112	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0098.ad.global	192.168.0.146	Rapid7 Insight Agents,AD_AMER
CLODIL0100.ad.global	192.168.101.8	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0103.ad.global	10.244.230.62	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0105.ad.global	192.168.1.87	Rapid7 Insight Agents,AD_AMER
CLODIL0106.ad.global	192.168.1.94	AD_AMER,Rapid7 Insight Agents
CLODIL0107.ad.global	192.168.0.8	AD_AMER,Rapid7 Insight Agents
CLODIL0108.ad.global	10.244.230.84	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODIL0111.ad.global	192.168.1.129	AD_AMER,Rapid7 Insight Agents
CLODIL0112.ad.global	192.168.100.25	AD_AMER,Rapid7 Insight Agents
CLODIL0114.ad.global	10.244.231.75	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0115.ad.global	10.244.231.97	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
CLODIL0116.ad.global	10.244.231.35	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall

Name	IP Address	Site
CLODIL0117.ad.global	192.168.100.10	AD_AMER,Rapid7 Insight Agents
CLODIL0118.ad.global	10.244.231.116	Rapid7 Insight Agents,AD_AMER
CLODIL0119.ad.global	10.244.230.91	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0120.ad.global	10.34.45.167	TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0123.ad.global	192.168.1.88	AD_AMER,Rapid7 Insight Agents
CLODIL0124.ad.global	10.244.231.106	AD_AMER,Rapid7 Insight Agents
CLODIL0138.ad.global	192.168.100.20	Rapid7 Insight Agents,AD_AMER
CLODIL0140.ad.global	10.244.231.67	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLODIL0142.ad.global	10.244.230.70	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLODIL0143.ad.global	10.244.231.85	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AD_AMER
CLODIL0144.ad.global	192.168.1.84	Rapid7 Insight Agents
CLODIL0148.ad.global	10.34.45.134	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0149.ad.global	192.168.1.104	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0155.ad.global	192.168.1.10	AD_AMER,Rapid7 Insight Agents
CLODIL0163.ad.global	10.244.231.83	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLSAND0007.ad.global	10.34.45.116	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLSAND0011.ad.global	10.34.45.130	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC
CLSAND0020.ad.global	10.244.231.48	AMER GLOBAL - UTC -6,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_A
CLSAND0024.ad.global	10.244.231.95	Rapid7 Insight Agents,TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
CLSAND0025.ad.global	10.244.230.62	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSAND0030.ad.global	192.168.100.7	Rapid7 Insight Agents,AD_AMER
CLSAND0031	10.34.45.131	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLSANL0003.ad.global	192.168.1.23	AD_AMER,Rapid7 Insight Agents
CLSANL0007.ad.global	192.168.1.89	Rapid7 Insight Agents,AD_AMER
CLSANL0016.ad.global	192.168.1.119	AD_AMER,Rapid7 Insight Agents
CLSANL0021.ad.global	192.168.1.147	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0028.ad.global	10.244.231.23	AMER GLOBAL - UTC -7,AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0032.ad.global	192.168.100.16	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLSANL0035.ad.global	192.168.1.16	AD_AMER,Rapid7 Insight Agents
CLSANL0040.ad.global	192.168.4.52	Rapid7 Insight Agents,AD_AMER
CLSANL0043.ad.global	192.168.100.2	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
CLSANL0045.ad.global	192.168.100.14	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,2020.12-Fireeye-NSA,AD_AMER,2021.02 - NSA-Fireeye
CLSANL0047.ad.global	192.168.1.85	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANL0052.ad.global	192.168.100.10	Rapid7 Insight Agents,AD_AMER
CLSANL0053.ad.global	10.34.45.143	Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
CLSANL0054.ad.global	10.34.45.107	TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE,2020.12-Fireeye-NSA,Rapid7 Insight Agents
CLSANL0055.ad.global	10.34.45.102	TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANL0056.ad.global	192.168.100.9	2021.02 - NSA-Fireeye,Rapid7 Insight Agents,AD_AMER,2020.12-Fireeye-NSA
CLSANL0057.ad.global	192.168.100.9	Rapid7 Insight Agents,AD_AMER
CLSANL0058.ad.global	192.168.0.131	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLSANL0059.ad.global	192.168.1.81	AD_AMER,Rapid7 Insight Agents
CLSANL0060.ad.global	192.168.1.10	Rapid7 Insight Agents,AD_AMER
CLSANL0061.ad.global	192.168.1.92	AD_AMER,Rapid7 Insight Agents
CLSANL0062.ad.global	192.168.100.5	Rapid7 Insight Agents,AD_AMER
CLSANL0064.ad.global	10.34.45.142	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_HID_AMER_APAC
CLSANL0067.ad.global	192.168.100.8	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_all_internall
CLSANL0070.ad.global	192.168.1.5	AD_AMER,Rapid7 Insight Agents
CLSANL0071.ad.global	10.244.230.114	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0072.ad.global	192.168.1.88	AD_AMER,Rapid7 Insight Agents
CLSANL0073.ad.global	192.168.1.19	Rapid7 Insight Agents,AD_AMER
CLSANL0074.ad.global	192.168.1.98	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0075.ad.global	10.244.231.104	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLSANL0076.ad.global	192.168.0.11	AD_AMER,Rapid7 Insight Agents
CLSANL0077.ad.global	10.244.231.39	AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,Rapid7 Insight Agents
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodid0007.ad.global	10.244.231.52	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEA,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AMER GLOBAL - UTC - 6,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
clsans-dcfacle.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0002.ad.global	10.244.229.100	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsansls0001.ad.global	10.244.229.11	AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers

Name	IP Address	Site
clsansts0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA- Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_ Log4Shell_all_internall,TI_Log4Shell_all_servers

9. Upgrade VMware ESXi to the latest version

Remediation Steps

Download and apply the upgrade from: <http://www.vmware.com/patchmgr/findPatchByReleaseName.portal>

The typical way to apply patches to VMware ESXi hosts is via the vCenter Update Manager. For details, see the vCenter Update Manager [Administration Guide](#).

To update ESX/ESXi hosts without using Update Manager, obtain the patch for this vulnerability by searching for the build number in the link below

<http://www.vmware.com/patchmgr/findPatchByReleaseName.portal>

Assets

Name	IP Address	Site
Unknown	10.244.230.49	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	10.244.230.49	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
Unknown	10.244.230.98	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.9	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA

10. Upgrade the CIFS authentication method

Remediation Steps

Upgrade the authentication method using the registry. Note that upgrading the authentication method to NTLMv2 will break compatibility with Windows 95/98/ME systems and older pre-NT4 SP4 systems. This behavior is by design. If the system itself is NT4 SP3 or earlier, it must be upgraded to at least NT4 SP4 before making these changes. Note that the settings described below can also be set via Group Policy, under "Security Options", "LAN Manager Authentication Level".

Run the registry editor (regedit.exe or regedt32.exe) and browse to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

and set the following value:

Value Name: LMCompatibilityLevel

Data Type: REG_DWORD

Data: Level 5 should be used.

The valid values are:

0

Send LM response and NTLM response; never use NTLMv2 session security

1

Use NTLMv2 session security if negotiated

2

Send NTLM authentication only

3

Send NTLMv2 authentication only

4

DC refuses LM authentication

5

DC refuses LM and NTLM authentication (accepts only NTLMv2)

You should also modify the following values to the highest levels:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\

Value Name: NtlmMinClientSec

Data Type: REG_DWORD

Data: See

[Security guidance for ntlmv1](https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication) (<https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication>) for details.

Value Name: NtlmMinServerSec

Data Type: REG_DWORD

Data: See

[Security guidance for ntlmv1](https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication) (<https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication>) for details.

You must then shut down and restart for the changes to take effect.

Assets

Name	IP Address	Site
CLODID0049.ad.global	10.244.231.166	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AD_A MER,Rapid7 Insight Agents
CLODID0050.ad.global	10.34.45.122	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC ,Rapid7 Insight Agents,AD_AMER
CLODID0053.ad.global	10.244.231.57	AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_inter nall,Rapid7 Insight Agents
CLODIL0078.ad.global	192.168.1.90	Rapid7 Insight Agents
CLODIL0107.ad.global	192.168.0.8	AD_AMER,Rapid7 Insight Agents
CLODIL0108.ad.global	10.244.230.84	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODIL0110.ad.global	192.168.0.12	AD_AMER,Rapid7 Insight Agents
CLODIL0111.ad.global	192.168.1.129	AD_AMER,Rapid7 Insight Agents
CLODIL0112.ad.global	192.168.100.25	AD_AMER,Rapid7 Insight Agents
CLODIL0114.ad.global	10.244.231.75	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER

Name	IP Address	Site
CLODIL0115.ad.global	10.244.231.97	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
CLODIL0116.ad.global	10.244.231.35	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLODIL0117.ad.global	192.168.100.10	AD_AMER,Rapid7 Insight Agents
CLODIL0118.ad.global	10.244.231.116	Rapid7 Insight Agents,AD_AMER
CLODIL0119.ad.global	10.244.230.91	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0120.ad.global	10.34.45.167	TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0121.ad.global	10.244.231.147	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0122.ad.global	192.168.1.102	Rapid7 Insight Agents,AD_AMER
CLODIL0123.ad.global	192.168.1.88	AD_AMER,Rapid7 Insight Agents
CLODIL0124.ad.global	10.244.231.106	AD_AMER,Rapid7 Insight Agents
CLODIL0125.ad.global	192.168.1.17	Rapid7 Insight Agents,AD_AMER
CLODIL0126.ad.global	192.168.1.141	Rapid7 Insight Agents
CLODIL0127.ad.global	192.168.0.14	Rapid7 Insight Agents
CLODIL0128.ad.global	192.168.173.116	AD_AMER,Rapid7 Insight Agents
CLODIL0130.ad.global	192.168.0.5	Rapid7 Insight Agents
CLODIL0131.ad.global	192.168.100.11	Rapid7 Insight Agents,AD_AMER
CLODIL0132.ad.global	192.168.8.102	Rapid7 Insight Agents
CLODIL0133.ad.global	192.168.140.102	Rapid7 Insight Agents
CLODIL0134.ad.global	192.168.0.9	Rapid7 Insight Agents
CLODIL0135.ad.global	192.168.100.46	Rapid7 Insight Agents
CLODIL0136.ad.global	192.168.1.8	Rapid7 Insight Agents
CLODIL0138.ad.global	192.168.100.20	Rapid7 Insight Agents,AD_AMER
CLODIL0139.ad.global	192.168.100.69	AD_AMER,Rapid7 Insight Agents
CLODIL0140.ad.global	10.244.231.67	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLODIL0141.ad.global	10.244.231.109	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AD_AMER
CLODIL0142.ad.global	10.244.230.70	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLODIL0143.ad.global	10.244.231.85	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AD_AMER
CLODIL0144.ad.global	192.168.1.84	Rapid7 Insight Agents
CLODIL0145.ad.global	192.168.100.33	Rapid7 Insight Agents,AD_AMER
CLODIL0146.ad.global	192.168.18.78	AD_AMER,Rapid7 Insight Agents
CLODIL0147.ad.global	10.244.230.76	Rapid7 Insight Agents,AD_AMER
CLODIL0148.ad.global	10.34.45.134	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0149.ad.global	192.168.1.104	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0150.ad.global	192.168.1.118	AD_AMER,Rapid7 Insight Agents
CLODIL0152.ad.global	192.168.18.51	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0154.ad.global	192.168.18.121	Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0155.ad.global	192.168.1.10	AD_AMER,Rapid7 Insight Agents
CLODIL0156.ad.global	192.168.1.110	AD_AMER,Rapid7 Insight Agents
CLODIL0157.ad.global	10.34.45.165	AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents

Name	IP Address	Site
CLODIL0158.ad.global	10.244.231.136	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0159.ad.global	10.244.230.43	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0160.ad.global	192.168.1.130	Rapid7 Insight Agents,AD_AMER
CLODIL0161.ad.global	10.244.231.103	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0162.ad.global	10.244.230.67	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0163.ad.global	10.244.231.83	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLSANAPPTTEST01	10.208.32.5	TI_Cloud,TI_Log4Shell_all_internall
CLSANDBTEST01	10.208.32.6	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Cloud
CLSANL0069.ad.global	192.168.0.5	Rapid7 Insight Agents,AD_AMER
CLSANL0070.ad.global	192.168.1.5	AD_AMER,Rapid7 Insight Agents
CLSANL0071.ad.global	10.244.230.114	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0072.ad.global	192.168.1.88	AD_AMER,Rapid7 Insight Agents
CLSANL0073.ad.global	192.168.1.19	Rapid7 Insight Agents,AD_AMER
CLSANL0074.ad.global	192.168.1.98	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0075.ad.global	10.244.231.104	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLSANL0076.ad.global	192.168.0.11	AD_AMER,Rapid7 Insight Agents
CLSANL0077.ad.global	10.244.231.39	AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,Rapid7 Insight Agents
CLSANL0078.ad.global	192.168.0.8	Rapid7 Insight Agents,AD_AMER
CLSANL0079.ad.global	192.168.0.34	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0080.ad.global	192.168.1.97	AD_AMER,Rapid7 Insight Agents
CLSANL0081.ad.global	192.168.1.11	AD_AMER,Rapid7 Insight Agents
CLSANL0083.ad.global	192.168.250.126	Rapid7 Insight Agents
CLSANL0085.ad.global	192.168.1.25	Rapid7 Insight Agents,AD_AMER
CLSANL0086.ad.global	192.168.1.98	Rapid7 Insight Agents,AD_AMER
CLSANL0087.ad.global	192.168.1.81	Rapid7 Insight Agents
CLSANL0088.ad.global	192.168.0.7	Rapid7 Insight Agents
CLSANL0089.ad.global	192.168.1.89	Rapid7 Insight Agents
CLSANL0090.ad.global	192.168.101.15	AD_AMER,Rapid7 Insight Agents
CLSANL0091.ad.global	192.168.1.61	Rapid7 Insight Agents,AD_AMER
CLSANL0092.ad.global	192.168.1.15	Rapid7 Insight Agents,AD_AMER
CLSANL0093.ad.global	192.168.0.64	Rapid7 Insight Agents,AD_AMER
CLSANL0094.ad.global	10.244.230.51	Rapid7 Insight Agents,AD_AMER
CLSANL0095.ad.global	192.168.0.158	Rapid7 Insight Agents,AD_AMER
CLSANL0096.ad.global	192.168.1.178	Rapid7 Insight Agents,AD_AMER
CLSANL0097.ad.global	192.168.100.125	Rapid7 Insight Agents,AD_AMER
CLSANL0098.ad.global	192.168.100.23	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0099.ad.global	10.34.45.173	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
bdc-bui-04.ad.global	10.244.229.3	TI_Log4Shell_all_servers,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsanl0068.ad.global	192.168.0.30	Rapid7 Insight Agents,AD_AMER
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AMER GLOBAL - UTC - 6,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
clsans-dcfacale.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall

Name	IP Address	Site
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0002.ad.global	10.244.229.100	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_
clsansls0001.ad.global	10.244.229.11	AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers
clsanstst0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers

11. Secure the SNMP installation

Remediation Steps

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

Assets

Name	IP Address	Site
18J162101364	10.34.45.41	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
18J162101365	10.34.45.43	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
18J162101746	10.34.45.42	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
18J162203455	10.34.45.46	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
18J162203458	10.34.45.45	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA
18J163302396	10.34.45.151	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
18J163600187	10.34.45.48	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
18J163701856	10.34.45.40	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall, AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
18J163801944	10.34.45.44	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.101	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.104	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Compact	10.34.45.106	AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.127	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Compact	10.34.45.128	AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.139	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.86	AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.87	AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.89	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Compact	10.34.45.90	AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.91	AMER GLOBAL - BRASIL/CHILE
Compact	10.34.45.93	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Compact	10.34.45.99	AMER GLOBAL - BRASIL/CHILE
EPSON2578E2	10.34.45.52	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
NPI39F4A9	10.244.231.63	AMER GLOBAL - BRASIL/CHILE
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP58387947630C	10.244.231.87	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
RNP58387966934F	10.34.45.17	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
SEC30CDA73E4967	10.244.230.205	AMER GLOBAL - UTC - 6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
SEC30CDA79DF539	10.244.230.208	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_internall,AMER GLOBAL - AMER GLOBAL -
SEC30CDA79DF566	10.34.45.50	BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
SEC30CDA79DF573	10.244.230.207	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6
SEC30CDA79DF5C4	10.244.230.204	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.114	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.156	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.158	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC
WindowsCE	10.34.45.98	AMER GLOBAL - BRASIL/CHILE
admin-vta.ad.global	10.34.45.54	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
npi2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall

12. 2022-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5013952)

Remediation Steps

Download and apply the patch from: <https://support.microsoft.com/kb/5013952> <https://support.microsoft.com/kb/5013952>

Assets

Name	IP Address	Site
CLODISDP0001.ad.global	10.244.231.176	TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE, AMER GLOBAL - UTC - 6, TI_Log4Shell_all_servers
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER, TI_Log4Shell_all_internall, AMER GLOBAL - UTC - 6, TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC, TI_all_AD_Divisional_Servers, AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA, AD_AMER, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, AMER GLOBAL - BRASIL/CHILE, TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, AD_AMER, TI_all_AD_Divisional_Servers
clsansis0001.ad.global	10.244.229.20	AD_AMER, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_all_internall, TI_all_AD_Divisional_Servers, TI_Log4Shell_all_servers, AMER GLOBAL - UTC -6, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE

13. Update McAfee Agent to version 5.7.6

Remediation Steps

Update McAfee Agent to version 5.7.6 from [here](#)

Assets

Name	IP Address	Site
CLODIL0001.ad.global	10.0.1.12	Rapid7 Insight Agents,AD_AMER
CLODIL0005.ad.global	192.168.0.7	Rapid7 Insight Agents,AD_AMER
CLODIL0006.ad.global	192.168.0.14	Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AD_AM
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0010.ad.global	192.168.1.100	AD_AAGS,Rapid7 Insight Agents
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0013.ad.global	10.244.231.93	2020.12-Fireeye-NSA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0014.ad.global	10.244.231.52	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0019.ad.global	192.168.18.4	AD_AMER,Rapid7 Insight Agents
CLODIL0021.ad.global	192.168.1.20	AD_AMER,Rapid7 Insight Agents
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0026.ad.global	192.168.0.6	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0027.ad.global	10.244.231.146	TI_Log4Shell_all_internall,AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0028.ad.global	192.168.1.122	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0036.ad.global	10.244.231.42	AD_AMER,2021.02 - NSA-Fireeye,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6
CLODIL0038.ad.global	10.244.231.94	AD_AMER,2020.12-Fireeye-NSA,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
CLODIL0044.ad.global	10.244.230.63	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0045.ad.global	192.168.1.118	Rapid7 Insight Agents,AD_AMER
CLODIL0048.ad.global	192.168.1.9	AD_AMER,Rapid7 Insight Agents
CLODIL0049.ad.global	192.168.0.110	Rapid7 Insight Agents,AD_AMER
CLODIL0054.ad.global	10.244.231.106	Rapid7 Insight Agents
CLODIL0056.ad.global	10.244.231.174	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0057.ad.global	192.168.70.12	AD_AMER,Rapid7 Insight Agents
CLODIL0058.ad.global	10.244.231.45	Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0059.ad.global	192.168.8.100	Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_EMEIA
CLODIL0063.ad.global	10.34.45.108	Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0064.ad.global	192.168.1.3	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC
CLODIL0065.ad.global	10.34.45.125	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0067.ad.global	192.168.45.93	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0068.ad.global	192.168.100.6	AD_AMER,Rapid7 Insight Agents
CLODIL0072.ad.global	192.168.43.132	AD_AMER,Rapid7 Insight Agents
CLODIL0073.ad.global	192.168.56.162	Rapid7 Insight Agents
CLODIL0076.ad.global	192.168.1.156	Rapid7 Insight Agents,AD_AMER

Name	IP Address	Site
CLODIL0078.ad.global	192.168.1.90	Rapid7 Insight Agents
CLODIL0082.ad.global	10.244.230.44	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0083.ad.global	10.34.45.105	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0085.ad.global	192.168.3.7	Rapid7 Insight Agents,AD_AMER
CLODIL0086.ad.global	10.244.230.52	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0087.ad.global	192.168.1.126	AD_AMER,Rapid7 Insight Agents
CLODIL0088.ad.global	10.244.231.81	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0092.ad.global	192.168.1.88	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0093.ad.global	192.168.0.4	AD_AMER,Rapid7 Insight Agents
CLODIL0094.ad.global	192.168.100.18	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0095.ad.global	10.244.231.91	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0096.ad.global	10.244.231.162	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0097.ad.global	10.34.45.112	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0098.ad.global	192.168.0.146	Rapid7 Insight Agents,AD_AMER
CLODIL0100.ad.global	192.168.101.8	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0103.ad.global	10.244.230.62	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0105.ad.global	192.168.1.87	Rapid7 Insight Agents,AD_AMER
CLODIL0106.ad.global	192.168.1.94	AD_AMER,Rapid7 Insight Agents
CLODIL0107.ad.global	192.168.0.8	AD_AMER,Rapid7 Insight Agents
CLODIL0108.ad.global	10.244.230.84	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEA
CLODIL0111.ad.global	192.168.1.129	AD_AMER,Rapid7 Insight Agents
CLODIL0112.ad.global	192.168.100.25	AD_AMER,Rapid7 Insight Agents
CLODIL0114.ad.global	10.244.231.75	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0115.ad.global	10.244.231.97	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
CLODIL0116.ad.global	10.244.231.35	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLODIL0117.ad.global	192.168.100.10	AD_AMER,Rapid7 Insight Agents
CLODIL0118.ad.global	10.244.231.116	Rapid7 Insight Agents,AD_AMER
CLODIL0119.ad.global	10.244.230.91	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0120.ad.global	10.34.45.167	TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0121.ad.global	10.244.231.147	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0122.ad.global	192.168.1.102	Rapid7 Insight Agents,AD_AMER
CLODIL0123.ad.global	192.168.1.88	AD_AMER,Rapid7 Insight Agents
CLODIL0124.ad.global	10.244.231.106	AD_AMER,Rapid7 Insight Agents
CLODIL0125.ad.global	192.168.1.17	Rapid7 Insight Agents,AD_AMER
CLODIL0126.ad.global	192.168.1.141	Rapid7 Insight Agents
CLODIL0127.ad.global	192.168.0.14	Rapid7 Insight Agents
CLODIL0128.ad.global	192.168.173.116	AD_AMER,Rapid7 Insight Agents
CLODIL0130.ad.global	192.168.0.5	Rapid7 Insight Agents
CLODIL0131.ad.global	192.168.100.11	Rapid7 Insight Agents,AD_AMER
CLODIL0132.ad.global	192.168.8.102	Rapid7 Insight Agents
CLODIL0133.ad.global	192.168.140.102	Rapid7 Insight Agents

Name	IP Address	Site
CLODIL0134.ad.global	192.168.0.9	Rapid7 Insight Agents
CLODIL0135.ad.global	192.168.100.46	Rapid7 Insight Agents
CLODIL0136.ad.global	192.168.1.8	Rapid7 Insight Agents
CLODIL0138.ad.global	192.168.100.20	Rapid7 Insight Agents,AD_AMER
CLODIL0139.ad.global	192.168.100.69	AD_AMER,Rapid7 Insight Agents
CLODIL0140.ad.global	10.244.231.67	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLODIL0141.ad.global	10.244.231.109	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AD_AMER
CLODIL0142.ad.global	10.244.230.70	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLODIL0143.ad.global	10.244.231.85	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AD_AMER
CLODIL0145.ad.global	192.168.100.33	Rapid7 Insight Agents,AD_AMER
CLODIL0146.ad.global	192.168.18.78	AD_AMER,Rapid7 Insight Agents
CLODIL0147.ad.global	10.244.230.76	Rapid7 Insight Agents,AD_AMER
CLODIL0148.ad.global	10.34.45.134	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0149.ad.global	192.168.1.104	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0150.ad.global	192.168.1.118	AD_AMER,Rapid7 Insight Agents
CLODIL0152.ad.global	192.168.18.51	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0154.ad.global	192.168.18.121	Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0155.ad.global	192.168.1.10	AD_AMER,Rapid7 Insight Agents
CLODIL0156.ad.global	192.168.1.110	AD_AMER,Rapid7 Insight Agents
CLODIL0157.ad.global	10.34.45.165	AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents
CLODIL0158.ad.global	10.244.231.136	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0159.ad.global	10.244.230.43	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0160.ad.global	192.168.1.130	Rapid7 Insight Agents,AD_AMER
CLODIL0161.ad.global	10.244.231.103	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0162.ad.global	10.244.230.67	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0163.ad.global	10.244.231.83	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0003.ad.global	192.168.1.23	AD_AMER,Rapid7 Insight Agents
CLSANL0007.ad.global	192.168.1.89	Rapid7 Insight Agents,AD_AMER
CLSANL0016.ad.global	192.168.1.119	AD_AMER,Rapid7 Insight Agents
CLSANL0021.ad.global	192.168.1.147	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0028.ad.global	10.244.231.23	AMER GLOBAL - UTC -7,AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0032.ad.global	192.168.100.16	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLSANL0035.ad.global	192.168.1.16	AD_AMER,Rapid7 Insight Agents
CLSANL0040.ad.global	192.168.4.52	Rapid7 Insight Agents,AD_AMER
CLSANL0043.ad.global	192.168.100.2	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0045.ad.global	192.168.100.14	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,2020.12-Fireeye-NSA,AD_AMER,2021.02 - NSA-Fireeye

Name	IP Address	Site
CLSANL0047.ad.global	192.168.1.85	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANL0049.ad.global	192.168.0.19	AD_AMER,Rapid7 Insight Agents
CLSANL0052.ad.global	192.168.100.10	Rapid7 Insight Agents,AD_AMER
CLSANL0053.ad.global	10.34.45.143	Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
CLSANL0054.ad.global	10.34.45.107	TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE,2020.12-Fireeye-NSA,Rapid7 Insight Agents
CLSANL0055.ad.global	10.34.45.102	TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANL0056.ad.global	192.168.100.9	2021.02 - NSA-Fireeye,Rapid7 Insight Agents,AD_AMER,2020.12-Fireeye-NSA
CLSANL0057.ad.global	192.168.100.9	Rapid7 Insight Agents,AD_AMER
CLSANL0058.ad.global	192.168.0.131	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLSANL0059.ad.global	192.168.1.81	AD_AMER,Rapid7 Insight Agents
CLSANL0060.ad.global	192.168.1.10	Rapid7 Insight Agents,AD_AMER
CLSANL0061.ad.global	192.168.1.92	AD_AMER,Rapid7 Insight Agents
CLSANL0062.ad.global	192.168.100.5	Rapid7 Insight Agents,AD_AMER
CLSANL0063.ad.global	192.168.1.84	AD_AMER,Rapid7 Insight Agents
CLSANL0064.ad.global	10.34.45.142	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_HID_AMER_APAC
CLSANL0067.ad.global	192.168.100.8	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER,TI_Log4Shell_all_internall
CLSANL0069.ad.global	192.168.0.5	Rapid7 Insight Agents,AD_AMER
CLSANL0070.ad.global	192.168.1.5	AD_AMER,Rapid7 Insight Agents
CLSANL0071.ad.global	10.244.230.114	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0072.ad.global	192.168.1.88	AD_AMER,Rapid7 Insight Agents
CLSANL0073.ad.global	192.168.1.19	Rapid7 Insight Agents,AD_AMER
CLSANL0074.ad.global	192.168.1.98	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0075.ad.global	10.244.231.104	AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLSANL0076.ad.global	192.168.0.11	AD_AMER,Rapid7 Insight Agents
CLSANL0077.ad.global	10.244.231.39	AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,Rapid7 Insight Agents
CLSANL0078.ad.global	192.168.0.8	Rapid7 Insight Agents,AD_AMER
CLSANL0079.ad.global	192.168.0.34	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0080.ad.global	192.168.1.97	AD_AMER,Rapid7 Insight Agents
CLSANL0081.ad.global	192.168.1.11	AD_AMER,Rapid7 Insight Agents
CLSANL0083.ad.global	192.168.250.126	Rapid7 Insight Agents
CLSANL0085.ad.global	192.168.1.25	Rapid7 Insight Agents,AD_AMER
CLSANL0086.ad.global	192.168.1.98	Rapid7 Insight Agents,AD_AMER
CLSANL0087.ad.global	192.168.1.81	Rapid7 Insight Agents
CLSANL0088.ad.global	192.168.0.7	Rapid7 Insight Agents
CLSANL0089.ad.global	192.168.1.89	Rapid7 Insight Agents
CLSANL0090.ad.global	192.168.101.15	AD_AMER,Rapid7 Insight Agents
CLSANL0091.ad.global	192.168.1.61	Rapid7 Insight Agents,AD_AMER
CLSANL0092.ad.global	192.168.1.15	Rapid7 Insight Agents,AD_AMER
CLSANL0093.ad.global	192.168.0.64	Rapid7 Insight Agents,AD_AMER
CLSANL0094.ad.global	10.244.230.51	Rapid7 Insight Agents,AD_AMER
CLSANL0095.ad.global	192.168.0.158	Rapid7 Insight Agents,AD_AMER
CLSANL0096.ad.global	192.168.1.178	Rapid7 Insight Agents,AD_AMER

Name	IP Address	Site
CLSANL0097.ad.global	192.168.100.125	Rapid7 Insight Agents,AD_AMER
CLSANL0098.ad.global	192.168.100.23	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0099.ad.global	10.34.45.173	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
clsanl0068.ad.global	192.168.0.30	Rapid7 Insight Agents,AD_AMER

14. Secure the FTP account

Remediation Steps

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

Assets

Name	IP Address	Site
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP58387947630C	10.244.231.87	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
RNP58387966934F	10.34.45.17	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.244.230.161	EMEA GLOBAL - FRANCE,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - SERVERS,EMEA GLOBAL - UK,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -7,TI_Log4Shell_EMEIA,AAAB - DC2.0 -
Unknown	10.244.230.161	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.114	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.156	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC
npi2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall

15. Obtain a new certificate from your CA and ensure the server configuration is correct

Remediation Steps

Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation. If a self-signed certificate is being used, consider obtaining a signed certificate from a CA.

References: [Mozilla: Connection Untrusted Error SSLShopper: SSL Certificate Not Trusted Error Windows/IIS certificate chain config](#) [Apache SSL config](#) [Nginx SSL config](#) [CertificateChain.io](#)

Assets

Name	IP Address	Site
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLODISDC0001.ad.global	10.244.229.240	AD_Domain_controllers,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
EPSON2578E2	10.34.45.52	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP58387947630C	10.244.231.87	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
RNP58387966934F	10.34.45.17	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.133.251.1	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.229.2	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - UTC -6
Unknown	10.244.230.1	AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall

Name	IP Address	Site
Unknown	10.244.230.101	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	10.244.230.153	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
Unknown	10.244.230.161	EMEA GLOBAL - FRANCE,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - SERVERS,EMEA GLOBAL - UK,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 7,TI_Log4Shell_EMEIA,AAAB - DC2.0 - AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	10.244.230.49	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
Unknown	10.244.230.98	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.107	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.118	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.12	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.120	AD_AMER,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.122	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.131	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.136	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.141	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.142	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.143	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.145	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.146	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.17	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.19	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.2	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_All_Linux,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.22	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.24	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.29	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.3	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_All_Linux
Unknown	10.244.231.31	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.1	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.162	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.164	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.34.45.3	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.31	TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
Unknown	10.34.45.32	TI_All_Linux,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.33	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_All_Linux
Unknown	10.34.45.34	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_All_Linux,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.35	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.4	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.6	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.7	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.9	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	200.111.184.179	AMER GLOBAL-External,TI_Log4Shell_external
Unknown	200.111.184.180	AMER GLOBAL-External,TI_Log4Shell_external
Unknown	200.111.184.183	AMER GLOBAL-External,TI_Log4Shell_external
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AMER,AMER GLOBAL - UTC -6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcfacele.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC -6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansls0001.ad.global	10.244.229.11	AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers
clsanstst0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers
npi2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall

16. Fix the subject's Common Name (CN) field in the certificate

Remediation Steps

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

Assets

Name	IP Address	Site
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
EPSON2578E2	10.34.45.52	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP58387947630C	10.244.231.87	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
RNP58387966934F	10.34.45.17	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.133.251.1	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.229.2	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - UTC -6
Unknown	10.244.230.1	AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.244.230.101	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	10.244.230.153	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
Unknown	10.244.230.161	EMEA GLOBAL - FRANCE,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - SERVERS,EMEA GLOBAL - UK,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -7,TI_Log4Shell_EMEIA,AAAB - DC2.0 -
Unknown	10.244.230.49	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA

Name	IP Address	Site
Unknown	10.244.230.49	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC-6,TI_Log4Shell_all_internall
Unknown	10.244.230.98	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.107	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.118	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.12	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.120	AD_AMER,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.122	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.131	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.136	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.141	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.142	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.143	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.145	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.146	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.17	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.19	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.2	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_All_Linux,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.22	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.24	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.29	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.3	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_All_Linux
Unknown	10.244.231.31	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.1	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.162	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.164	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.34.45.3	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.31	TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.32	TI_All_Linux,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.33	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_All_Linux
Unknown	10.34.45.34	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_All_Linux,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.35	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
Unknown	10.34.45.4	TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.6	TI_Log4Shell_all_internall, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.7	TI_Log4Shell_all_internall, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.9	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_EMEIA
Unknown	200.111.184.179	AMER GLOBAL-External, TI_Log4Shell_external
Unknown	200.111.184.180	AMER GLOBAL-External, TI_Log4Shell_external
Unknown	200.111.184.183	AMER GLOBAL-External, TI_Log4Shell_external
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers, TI_Log4Shell_all_internall, TI_Log4Shell_HID_AMER_APAC, AD_AMER, TI_all_AD_Divisional_Servers, TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall, AD_AMER, TI_all_AD_Divisional_Servers, AMER GLOBAL - UTC - 6, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - BRASIL/CHILE
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC, TI_all_AD_Divisional_Servers, AMER GLOBAL - BRASIL/CHILE, AD_AMER, TI_Log4Shell_all_internall
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA, TI_all_AD_Divisional_Servers, AD_AMER, TI_Log4Shell_all_internall, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_all_servers
clsansls0001.ad.global	10.244.229.11	AD_AMER, TI_Log4Shell_all_servers, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC, TI_Log4Shell_all_internall, TI_all_AD_Divisional_Servers

17. Upgrade to the latest version of Google Chrome

Remediation Steps

Install latest version of Google Chrome from the [Google Chrome](#) page.

Assets

Name	IP Address	Site
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0010.ad.global	192.168.1.100	AD_AAGS,Rapid7 Insight Agents
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0105.ad.global	192.168.1.87	Rapid7 Insight Agents,AD_AMER
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODIL0110.ad.global	192.168.0.12	AD_AMER,Rapid7 Insight Agents
CLODIL0141.ad.global	10.244.231.109	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AD_AMER
CLSAND0031	10.34.45.131	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers

18. 2022-04 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB5012649)

Remediation Steps

Download and apply the patch from: <https://support.microsoft.com/kb/5012649> <https://support.microsoft.com/kb/5012649>

Assets

Name	IP Address	Site
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
clsans-dcfacale.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC -6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER

19. Configure SMB signing for Windows

Remediation Steps

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see [this Microsoft article](#) for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

Assets

Name	IP Address	Site
CLODID0055	10.34.45.169	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
CLODID0056	10.34.45.177	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
CLODID0057	10.34.45.175	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0092.ad.global	192.168.1.88	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0094.ad.global	192.168.100.18	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0095.ad.global	10.244.231.91	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0111.ad.global	192.168.1.129	AD_AMER,Rapid7 Insight Agents
CLODIL0154.ad.global	192.168.18.121	Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0157.ad.global	10.34.45.165	AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,Rapid7 Insight Agents
CLODIL0158.ad.global	10.244.231.136	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0161.ad.global	10.244.231.103	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0162.ad.global	10.244.230.67	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLODIL0163.ad.global	10.244.231.83	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLODISDP0001.ad.global	10.244.231.176	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers
CLSANAPPTTEST01	10.208.32.5	TI_Cloud,TI_Log4Shell_all_internall
CLSAND0043	10.34.45.172	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLSANDBTEST01	10.208.32.6	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Cloud
CLSANL0021.ad.global	192.168.1.147	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0056.ad.global	192.168.100.9	2021.02 - NSA-Fireeye,Rapid7 Insight Agents,AD_AMER,2020.12-Fireeye-NSA
CLSANL0098.ad.global	192.168.100.23	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0099.ad.global	10.34.45.173	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
bdc-bui-04.ad.global	10.244.229.3	TI_Log4Shell_all_servers,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AMER GLOBAL - UTC - 6,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
clsans-dcfacale.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall

Name	IP Address	Site
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0002.ad.global	10.244.229.100	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_
clsansls0001.ad.global	10.244.229.11	AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers
clsanststs0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers

20. Disable HTTP OPTIONS method

Remediation Steps

Disable HTTP OPTIONS method on your web server. Refer to your web server's instruction manual on how to do this.

Web servers that respond to the OPTIONS HTTP method expose what other methods are supported by the web server, allowing attackers to narrow and intensify their efforts.

Assets

Name	IP Address	Site
CLODID0015.ad.global	10.34.45.154	TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC - 6,2020.12-Fireeye-NSA,AD_AMER,Rapid7 Insight Agents
CLODID0020.ad.global	10.34.45.140	TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_EMEIA,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODID0033.ad.global	10.244.230.21	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODID0043.ad.global	10.244.231.195	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,Rapid7 Insight Agents
CLODID0045.ad.global	10.244.231.14	AD_AMER,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC - 7,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,Rapid7 Insight Agents
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0014.ad.global	10.244.231.52	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0027.ad.global	10.244.231.146	TI_Log4Shell_all_internall,AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLODIL0028.ad.global	192.168.1.122	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0036.ad.global	10.244.231.42	AD_AMER,2021.02 - NSA-Fireeye,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6
CLODIL0038.ad.global	10.244.231.94	AD_AMER,2020.12-Fireeye-NSA,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall
CLODIL0044.ad.global	10.244.230.63	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0056.ad.global	10.244.231.174	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0063.ad.global	10.34.45.108	Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0065.ad.global	10.34.45.125	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLSANAPPTTEST01	10.208.32.5	TI_Cloud,TI_Log4Shell_all_internall
CLSAND0007.ad.global	10.34.45.116	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLSAND0011.ad.global	10.34.45.130	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
CLSAND0020.ad.global	10.244.231.48	AMER GLOBAL - UTC -6,Rapid7 Insight Agents,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_A
CLSAND0025.ad.global	10.244.230.62	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSAND0031	10.34.45.131	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,TI_Log4Shell_all_internall
CLSANL0021.ad.global	192.168.1.147	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLSANL0032.ad.global	192.168.100.16	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLSANL0043.ad.global	192.168.100.2	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0045.ad.global	192.168.100.14	TI_Log4Shell_all_internall,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,2020.12-Fireeye-NSA,AD_AMER,2021.02 - NSA-Fireeye
CLSANL0047.ad.global	192.168.1.85	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_A
CLSANSAP0008	10.244.229.41	MER_APAC,TI_all_AD_Divisional_Servers,AME R GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AM ER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
NPI39F4A9	10.244.231.63	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Sh ell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_all_AD_Divisional _Servers,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.63	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.229.2	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log 4Shell_EMEIA,AMER GLOBAL - UTC -6
Unknown	10.244.230.154	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_ all_internall,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA
Unknown	10.244.230.157	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log 4Shell_HID_AMER_APAC
Unknown	10.244.231.107	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.118	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.12	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.120	AD_AMER,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.122	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.131	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.136	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.141	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.142	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.143	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.145	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.146	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.17	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.19	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.2	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AM ER_APAC,TI_All_Linux,TI_Log4Shell_EMEIA,AM ER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.22	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.24	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.29	AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
Unknown	10.244.231.3	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_All_Linux
Unknown	10.244.231.31	AMER GLOBAL - BRASIL/CHILE
bdc-bui-04.ad.global	10.244.229.3	TI_Log4Shell_all_servers,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_internall,TI_Log4Shell_HID_A MER_APAC,AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC ,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodid0007.ad.global	10.244.231.52	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
clodid0008.ad.global	10.244.231.42	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC ,AD_AMER,TI_Log4Shell_all_internall
clodid0023.ad.global	10.244.231.83	AMER GLOBAL - BRASIL/CHILE,AD_AMER
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AM ER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AM ER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_intern all,TI_Log4Shell_HID_AMER_APAC,AD_AMER, TI_all_AD_Divisional_Servers,TI_Log4Shell_EME IA,AMER GLOBAL - BRASIL/CHILE
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_ AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD _AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_A MER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_ Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log 4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers
clsans-dcfacale.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall, AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log 4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log 4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA, TI_Log4Shell_all_servers,TI_all_AD_Divisional_S ervers,AMER GLOBAL - UTC -6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AM ER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_inter nall
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Serv ers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC ,TI_Log4Shell_all_servers
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_ Log4Shell_all_internall,TI_all_AD_Divisional_Ser vers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL -
clsansls0001.ad.global	10.244.229.11	BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers
clsansts0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers

21. Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled

Remediation Steps

There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.

Assets

Name	IP Address	Site
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLODISDC0001.ad.global	10.244.229.240	AD_Domain_controllers,TI_Log4Shell_all_servers ,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
CLSANAPPTTEST01	10.208.32.5	TI_Cloud,TI_Log4Shell_all_internall
CLSANDBTEST01	10.208.32.6	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Cloud
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
EPSON2578E2	10.34.45.52	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA, AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.133.251.1	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.230.1	AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.244.230.153	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC ,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
Unknown	10.244.230.49	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	10.244.230.49	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
Unknown	10.244.230.98	AMER GLOBAL - BRASIL/CHILE

Name	IP Address	Site
Unknown	10.244.231.107	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.118	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.12	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.120	AD_AMER,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.122	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.131	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.136	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.141	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.142	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.143	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.145	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.146	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.17	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.19	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.22	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.24	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.29	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.31	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.1	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.162	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.3	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.31	TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.32	TI_All_Linux,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.33	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_All_Linux
Unknown	10.34.45.34	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_All_Linux,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.35	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.4	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.6	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.7	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.9	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	200.111.184.180	AMER GLOBAL-External,TI_Log4Shell_external

Name	IP Address	Site
Unknown	200.111.184.183	AMER GLOBAL-External,TI_Log4Shell_external
bdc-bui-04.ad.global	10.244.229.3	TI_Log4Shell_all_servers,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodid0007.ad.global	10.244.231.52	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AMER GLOBAL - UTC - 6,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
clsans-dcfacale.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall

Name	IP Address	Site
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0002.ad.global	10.244.229.100	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_
clsansls0001.ad.global	10.244.229.11	AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers
clsanstst0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers
np2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall

22. Disable TLS/SSL support for static key cipher suites

Remediation Steps

Configure the server to disable support for static key cipher suites.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](#) for instructions on disabling static key cipher suites. The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

Assets

Name	IP Address	Site
CLODID0043.ad.global	10.244.231.195	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_ EMEIA,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,Rapid7 Insight Agents
CLODIL0008.ad.global	192.168.250.36	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0012.ad.global	192.168.0.8	AMER GLOBAL - BRASIL/CHILE,AD_AMER,Rapid7 Insight Agents
CLODIL0028.ad.global	192.168.1.122	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0056.ad.global	10.244.231.174	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLODIL0094.ad.global	192.168.100.18	Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE,AD_AMER
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_ EMEIA
CLODIL0111.ad.global	192.168.1.129	AD_AMER,Rapid7 Insight Agents
CLODISAP0002.ad.global	10.244.231.5	TI_Log4Shell_all_internall,TI_Log4Shell_ EMEIA, TI_all_AD_Divisional_Servers,AD_AMER,TI_Log 4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers
CLODISDC0001.ad.global	10.244.229.240	AD_Domain_controllers,TI_Log4Shell_all_servers ,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
CLSANAPPTTEST01	10.208.32.5	TI_Cloud,TI_Log4Shell_all_internall
CLSANDBTEST01	10.208.32.6	TI_Log4Shell_all_servers,TI_Log4Shell_all_intern all,TI_Log4Shell_HID_AMER_APAC,TI_Cloud
CLSANL0043.ad.global	192.168.100.2	AD_AMER,Rapid7 Insight Agents,AMER GLOBAL - BRASIL/CHILE
CLSANL0058.ad.global	192.168.0.131	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLSANSAP0002.ad.global	10.244.231.6	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_A MER_APAC,TI_all_AD_Divisional_Servers,AME R GLOBAL - BRASIL/CHILE
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AM ER_APAC,AD_AMER,AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall,AD_AMER,TI_Log4Sh ell_HID_AMER_APAC,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_all_AD_Divisional _Servers,AMER GLOBAL - BRASIL/CHILE
EPSON2578E2	10.34.45.52	TI_Log4Shell_all_internall,TI_Log4Shell_ EMEIA, AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
RNP5838790C2156	10.244.231.37	TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
RNP583879459C0C	10.244.231.86	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
RNP583879459C14	10.244.230.210	TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.133.251.1	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.229.2	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - UTC -6
Unknown	10.244.230.1	AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.244.230.153	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
Unknown	10.244.230.49	AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	10.244.230.49	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC -6,TI_Log4Shell_all_internall
Unknown	10.244.230.98	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.107	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.118	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.12	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.120	AD_AMER,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.122	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.131	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.136	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.141	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.142	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.143	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.145	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.146	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.17	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.19	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.2	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_All_Linux,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.22	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.24	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.29	AMER GLOBAL - BRASIL/CHILE
Unknown	10.244.231.3	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_All_Linux
Unknown	10.244.231.31	AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.1	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.16	TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC

Name	IP Address	Site
Unknown	10.34.45.162	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA
Unknown	10.34.45.164	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall
Unknown	10.34.45.3	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.31	TI_All_Linux,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.32	TI_All_Linux,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.33	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_All_Linux
Unknown	10.34.45.34	TI_Log4Shell_EMEIA,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_All_Linux,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.35	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,TI_All_Linux,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.4	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
Unknown	10.34.45.6	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.7	TI_Log4Shell_all_internall,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
Unknown	10.34.45.9	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
Unknown	200.111.184.180	AMER GLOBAL-External,TI_Log4Shell_external
Unknown	200.111.184.183	AMER GLOBAL-External,TI_Log4Shell_external
bdc-bui-04.ad.global	10.244.229.3	TI_Log4Shell_all_servers,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
bdc-bui-sap.ad.global	10.244.229.10	TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall
clodid0007.ad.global	10.244.231.52	AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE
clodisap0005.ad.global	10.244.229.14	TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers
clodisap0006.ad.global	10.244.231.10	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clodisdb0001.ad.global	10.34.45.12	TI_Log4Shell_EMEIA,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers

Name	IP Address	Site
clodisis0003.ad.global	10.244.231.9	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers
clodisls0001.ad.global	10.244.229.30	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AD_AMER,AMER GLOBAL - UTC - 6,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-appprodu.ad.global	10.244.229.23	TI_Log4Shell_all_internall,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC - 6,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE
clsans-dcaxprod.ad.global	10.244.229.104	TI_all_AD_Divisional_Servers,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,TI_Log4Shell_all_servers
clsans-dcaxsql.ad.global	10.244.229.103	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,AMER GLOBAL - UTC - 6,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall
clsans-dcfacle.ad.global	10.244.229.26	TI_Log4Shell_EMEIA,TI_Log4Shell_all_internall,AD_AMER,AMER GLOBAL - UTC - 6,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC
clsans-wms01.ad.global	10.244.229.22	AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_EMEIA,TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,AMER GLOBAL - UTC -6,AD_AMER
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_all_internall
clsansdb0002.ad.global	10.244.229.13	TI_Log4Shell_EMEIA,TI_all_AD_Divisional_Servers,AD_AMER,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_servers
clsansfs0001.ad.global	10.244.229.24	TI_Log4Shell_all_servers,TI_all_AD_Divisional_Servers,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,AMER GLOBAL - UTC -6
clsansis0001.ad.global	10.244.229.20	AD_AMER,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_servers,AMER GLOBAL - UTC -6,TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE
clsansis0002.ad.global	10.244.229.100	TI_Log4Shell_all_servers,TI_Log4Shell_all_internall,TI_Log4Shell_HID_AMER_APAC,AD_AMER,TI_all_AD_Divisional_Servers,AMER GLOBAL - BRASIL/CHILE
clsansis0003.ad.global	10.244.229.21	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_all_internall,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_servers,TI_Log4Shell_HID_AMER_APAC,TI_all_AD_Divisional_AD_AMER,TI_Log4Shell_all_servers,AMER GLOBAL -
clsansls0001.ad.global	10.244.229.11	BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC,TI_Log4Shell_all_internall,TI_all_AD_Divisional_Servers

Name	IP Address	Site
clsansts0001.ad.global	10.244.229.27	AD_AMER,2021.02 - NSA-Fireeye,TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - BRASIL/CHILE,TI_all_AD_Divisional_Servers,TI_Log4Shell_all_internall,TI_Log4Shell_all_servers
npi2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC,AMER GLOBAL - UTC -6,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_all_internall

23. Upgrade to the latest version of Microsoft Edge

Remediation Steps

Upgrade to the latest version of Microsoft Edge [here](#). Alternatively, navigate to [About Microsoft Edge](#) (edge://settings/help) and select Download and install. Restart Edge once the update is installed.

Assets

Name	IP Address	Site
CLODID0015.ad.global	10.34.45.154	TI_Log4Shell_EMEIA,AMER GLOBAL - BRASIL/CHILE,AMER GLOBAL - UTC - 6,2020.12-Fireeye-NSA,AD_AMER,Rapid7 Insight Agents
CLODIL0006.ad.global	192.168.0.14	Rapid7 Insight Agents,TI_Log4Shell_HID_AMER_APAC,AD_AM
CLODIL0022.ad.global	192.168.0.101	Rapid7 Insight Agents,AD_AAGS,AMER GLOBAL - BRASIL/CHILE
CLODIL0068.ad.global	192.168.100.6	AD_AMER,Rapid7 Insight Agents
CLODIL0076.ad.global	192.168.1.156	Rapid7 Insight Agents,AD_AMER
CLODIL0086.ad.global	10.244.230.52	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLODIL0109.ad.global	10.244.231.78	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_EMEIA
CLODIL0110.ad.global	192.168.0.12	AD_AMER,Rapid7 Insight Agents
CLODIL0131.ad.global	192.168.100.11	Rapid7 Insight Agents,AD_AMER
CLODIL0140.ad.global	10.244.231.67	Rapid7 Insight Agents,AD_AMER,AMER GLOBAL - BRASIL/CHILE,TI_Log4Shell_HID_AMER_APAC
CLODIL0144.ad.global	192.168.1.84	Rapid7 Insight Agents
CLSANL0007.ad.global	192.168.1.89	Rapid7 Insight Agents,AD_AMER
CLSANL0018.ad.global	10.244.230.29	AD_AMER,AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents
CLSANL0035.ad.global	192.168.1.16	AD_AMER,Rapid7 Insight Agents
CLSANL0058.ad.global	192.168.0.131	AMER GLOBAL - BRASIL/CHILE,Rapid7 Insight Agents,AD_AMER
CLSANL0069.ad.global	192.168.0.5	Rapid7 Insight Agents,AD_AMER
CLSANL0092.ad.global	192.168.1.15	Rapid7 Insight Agents,AD_AMER

24. 2022-05 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5013942)

Remediation Steps

Download and apply the patch from: <https://support.microsoft.com/kb/5013942> <https://support.microsoft.com/kb/5013942>

Assets

Name	IP Address	Site
CLODIL0145.ad.global	192.168.100.33	Rapid7 Insight Agents,AD_AMER
CLSANL0083.ad.global	192.168.250.126	Rapid7 Insight Agents
CLSANL0089.ad.global	192.168.1.89	Rapid7 Insight Agents
CLSANL0094.ad.global	10.244.230.51	Rapid7 Insight Agents,AD_AMER

25. Upgrade to the latest version of OpenSSL

Remediation Steps

Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-3.0.3.tar.gz>

The latest version of OpenSSL is 3.0.3.

<http://ftp.openssl.org/source/openssl-3.0.3.tar.gz>

Assets

Name	IP Address	Site
CLSANSAP0008	10.244.229.41	TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC, AD_AMER, AMER GLOBAL - BRASIL/CHILE
CLSANSRF0001.ad.global	10.244.231.15	TI_Log4Shell_all_internall, AD_AMER, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - UTC - 6, TI_Log4Shell_all_servers, TI_all_AD_Divisional_Servers, AMER GLOBAL - BRASIL/CHILE
NPI23C96B	10.244.230.214	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_internall, AMER GLOBAL - UTC - 6
Unknown	10.244.230.153	AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - UTC - 6, TI_Log4Shell_EMEIA, TI_Log4Shell_all_internall
clsansap0008.ad.global	10.244.229.41	TI_Log4Shell_all_servers, TI_Log4Shell_HID_AMER_APAC, TI_all_AD_Divisional_Servers, AMER GLOBAL - BRASIL/CHILE, AD_AMER, TI_Log4Shell_all_internall
mpi2ca232.ad.global	10.244.231.220	TI_Log4Shell_HID_AMER_APAC, AMER GLOBAL - UTC - 6, AMER GLOBAL - BRASIL/CHILE, TI_Log4Shell_all_internall