



## Apache Log4j Updates



CBTS continues to review our products and vendors and is mitigating vulnerabilities as remediations become available. This is a fluid situation and we will continue to update this table as progress is made.

| SERVICE   | STATUS PER VENDOR                 | VENDOR RESOURCES  |
|---|-----------------------------------|---|
| Avaya Managed Telephony                         | Impacted, remediation in progress | <a href="https://support.avaya.com/helpcenter/getGenericDetails?detailId=1399839287609">https://support.avaya.com/helpcenter/getGenericDetails?detailId=1399839287609</a>   |
| Emerge  | Not Impacted                      |   |
| Evantage  | Not Impacted                      |   |
| HECC – Hosted Enterprise Contact Center         | Impacted, remediation in progress | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |
| HEUC - Hosted Enterprise Unified Communications | Impacted, remediation in progress | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |
| Hosted UC - Hosted Unified Communications       | Impacted, remediation implemented | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |
| Managed Backup - Bocada                         | Not Impacted                      | <a href="https://bocada-support.force.com/s/article/Bocada-does-not-use-Apache-Log4J-regarding-CVE-2021-44228-Vulnerability">https://bocada-support.force.com/s/article/Bocada-does-not-use-Apache-Log4J-regarding-CVE-2021-44228-Vulnerability</a>                     |
| Managed Backup - Commvault                      | Impacted, remediation implemented | <a href="https://community.commvault.com/search?q=log4j">https://community.commvault.com/search?q=log4j</a>   |
| Managed Backup - Veeam                          | Not Impacted                      | <a href="https://www.veeam.com/kb4254">https://www.veeam.com/kb4254</a>   |
| Managed Endpoint Protection (Trend)             | Not Impacted                      | <a href="https://success.trendmicro.com/solution/000289940">https://success.trendmicro.com/solution/000289940</a>   |
| Managed Load Balancing (F5)                     | Not Impacted                      | <a href="https://support.f5.com/csp/article/K19026212">https://support.f5.com/csp/article/K19026212</a>   |
| Managed patching - BigFix                       | Not Impacted                      | <a href="https://support.hcltechsw.com/csm/en?id=kb_article&amp;sysparm_article=KB0095486">https://support.hcltechsw.com/csm/en?id=kb_article&amp;sysparm_article=KB0095486</a>   |
| Managed patching - Ivanti                       | Not Impacted                      | <a href="https://forums.ivanti.com/s/article/CVE-2021-44228-Java-logging-library-log4j-Ivanti-Products-Impact-Mapping?language=en_US">https://forums.ivanti.com/s/article/CVE-2021-44228-Java-logging-library-log4j-Ivanti-Products-Impact-Mapping?language=en_US</a>   |
| MDR (Alert Logic)                               | Not Impacted                      | <a href="https://support.alertlogic.com/hc/en-us/articles/4412577028251-12-10-2021-Apache-Log4j-2-Remote-Code-Execution-Vulnerability">https://support.alertlogic.com/hc/en-us/articles/4412577028251-12-10-2021-Apache-Log4j-2-Remote-Code-Execution-Vulnerability</a> |
| Microsoft Teams Voice                           | Not Impacted                      | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-44228">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-44228</a>   |
| Monitoring - LogicMonitor                       | Impacted, remediation implemented | <a href="https://www.logicmonitor.com/support/log4shell-security-vulnerability-cve-2021-44228">https://www.logicmonitor.com/support/log4shell-security-vulnerability-cve-2021-44228</a>   |
| Monitoring – SL1                                | Not Impacted                      | <a href="https://support.sciencelogic.com/s/article/7061">https://support.sciencelogic.com/s/article/7061</a>   |
| NaaS - Meraki                                   | Not Impacted                      | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |



## Apache Log4j Updates



| SERVICE                                 | STATUS PER VENDOR                 | VENDOR RESOURCES  |
|---|-----------------------------------|---|
| NaaS - Bandwidth Aggregation - Meraki   | Not Impacted                      | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |
| NaaS - Circuit LOA - Meraki             | Not Impacted                      | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |
| NaaS - Managed LTE- Meraki              | Not Impacted                      | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd</a>   |
| Proofpoint Essentials                   | Impacted, remediation implemented | <a href="https://www.proofpoint.com/us/blog/corporate-news/proofpoints-response-log4j-vulnerability">https://www.proofpoint.com/us/blog/corporate-news/proofpoints-response-log4j-vulnerability</a>   |
| Ribbon – Sonus                          | Impacted, remediation in progress | <a href="https://support.sonus.net/pages/viewpage.action?spaceKey=ALLDOC&amp;title=CVE-2021-44228%3A+Critical+Apache+Log4j+Remote+Code+Execution+Vulnerability">https://support.sonus.net/pages/viewpage.action?spaceKey=ALLDOC&amp;title=CVE-2021-44228%3A+Critical+Apache+Log4j+Remote+Code+Execution+Vulnerability</a>               |
| SD-WAN-CheckPoint Harmony               | Not Impacted                      | <a href="https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&amp;solutionid=sk176865&amp;partition=General&amp;product=IPS">https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&amp;solutionid=sk176865&amp;partition=General&amp;product=IPS</a> |
| SD-WAN-VeloCloud                        | Impacted, remediation implemented | <a href="https://kb.vmware.com/s/article/87158">https://kb.vmware.com/s/article/87158</a>   |
| ServiceNow NOW                          | Not Impacted                      | <a href="https://community.servicenow.com/community?id=community_question&amp;sys_id=9f0798fedb144d5439445ac2ca9619d6">https://community.servicenow.com/community?id=community_question&amp;sys_id=9f0798fedb144d5439445ac2ca9619d6</a>   |
| SIP Trunking                            | Not Impacted                      |   |
| VDC (VMWare)                            | Impacted, remediation in progress | <a href="https://www.vmware.com/security/advisories/VMSA-2021-0028.html">https://www.vmware.com/security/advisories/VMSA-2021-0028.html</a>   |
| Vulnerability Scanning – Tenable Nessus | Not Impacted                      | <a href="https://www.tenable.com/log4j">https://www.tenable.com/log4j</a>   |

Not Impacted = product is not vulnerable to Log4j issues

Impacted, remediation implemented = product used a version of the Log4j software identified as vulnerable and the recommended mitigation has been implemented

Impacted, remediation in progress = product used a version of the Log4j software identified as vulnerable and the recommended mitigation is in process

Under Investigation = reviewing vendor information and impacts to different versions