# Apache vulnerabilities and impact on Amulet Hotkey products

Dec 15, 2021

*Last updated: 15 December 2021 18:00 PM Eastern Time*

New security vulnerabilities that can exploit Apache Log4j have been disclosed by security researchers on Dec 10, 2021. Please read this notice and the relevant advisories carefully to understand the risks and resolution steps that you may need, or may want, to make within your organization. Amulet Hotkey is working with technology partners to investigate potential impact to our products. This notice will be updated as information becomes available.

***Special note:*** *At this time Amulet Hotkey have not found any evidence that the DXZ zero client and remote workstation card products are affected by this vulnerability. See below for more information.*

## Vulnerabilities

| | |
|---|---|
| **Apache Log4j 2** | Denial of service attack NVD:CVE-2021-45046 Mitre:CVE-2021-45046 |
| **Mechanism for triggering** | The CVE-2021-44228 fix was incomplete in certain configurations which allows attackers with control over Thread Context Map input data to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack |
| **Affected platforms** | Any system using open source Apache Log4j2 software version 2.15.0 or lower. |
| **Systems affected** | Web servers and applications with web interfaces. |
| **Difficulty of successful attack** | CVSS Base Score: 3.7 Low<br>CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L |

| | |
|---|---|
| **Apache Log4j 2** | Remote Code Execution NVD:CVE-2021-44288 Mitre:CVE-2021-44228 |
| **Mechanism for triggering** | An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution has been enabled |
| **Affected platforms** | Any system using open source Apache Log4j2 software version 2.14.1 or lower. |
| **Systems affected** | Web servers and applications with web interfaces. |
| **Difficulty of successful attack** | CVSS Base Score: 10.0 Critical<br>CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H |

| | |
|---|---|
| **Apache Log4j 2** | Remote code execution NVD:CVE-2017-5645 Mitre:CVE-2017-5645 |
| **Mechanism for triggering** | When using the TCP or UDP socket server to receive serialized log events from another application, a specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code. |
| **Affected platforms** | Any system using open source Apache Log4j 2 software version 2.8.2 or lower. |
| **Systems affected** | Web servers and applications with web interfaces. |
| **Difficulty of successful attack** | CVSS Base Score: 9.8 Critical<br>CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

| | |
|---|---|
| **Apache Log4j 1 (EOL)** | Deserialization of untrusted data NVD:CVE-2021-4104 Mitre:CVE-2021-4104 |
| **Mechanism for triggering** | A remote attacker can execute code on the server if the deployed application is configured to use JMSAppender and to the attacker's JMS Broker. |
| **Affected platforms** | Any system using Apache Log4j version 1.x configured to use JMSAppender, or when the attacker has write access to the Log4j configuration for adding JMSAppender to the attacker's JMS Broker |
| **Systems affected** | Web servers and applications with web interfaces. |
| **Difficulty of successful attack** | CVSS Base Score: 6.6 Medium<br>CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |

| | |
|---|---|
| **Apache Log4j 1 (EOL)** | SocketServer deserialization of untrusted data NVD:CVE-2019-17571 Mitre:CVE-2019-17571 |
| **Mechanism for triggering** | Deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. |
| **Affected platforms** | Any system using open source Apache Log4j software version 1.2 to 1.2.17 |
| **Systems affected** | Web servers and applications with web interfaces. |
| **Difficulty of successful attack** | CVSS Base Score: 9.8 Critical<br>CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

| | |
|---|---|
| **Apache Log4j 1 (EOL)** | Improper certificate validation log message leak NVD:CVE-2020-9488 Mitre:CVE-2020-9488 |
| **Mechanism for triggering** | A certificate host mismatch could allow an SMTPS connection to be intercepted by a man-in-the-middle attack and leak log messages sent. |
| **Affected platforms** | Any system using open source Apache Log4j SMTP appender |
| **Systems affected** | Web servers and applications with web interfaces. |
| **Difficulty of successful attack** | CVSS Base Score: 3.7 Low<br>CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N |

## Solution

Amulet Hotkey products can incorporate components, products and technology from partners. We encourage customers to review vendor advisories and take the appropriate actions to mitigate these vulnerabilities. The tables below list some of the partner products used in Amulet Hotkey products and links to some of the vendor guidance.

**General vendor guidance:**

- **Modify Log4j:** Modify Log4j 2 for systems that need to use Log4j version 2 to 2.14.1. Modify Log4j 1 or adjust access for the OS user for systems that need to use Log4j 1.x. See vendor guidance for more information.
- **Apply updates:** Operating system, hypervisor and application software updates mitigate these attacks. We recommend that you closely review all vendor guidance related to your environment.
- **Solution impact:** Updates to mitigate these attacks may impact other software/firmware versions required in your environment. For example, updating VMware Horizon components may have dependencies on Teradici firmware versions etc. We recommend that you monitor critical systems accordingly.

Table 1: Amulet Hotkey Products and Solution Partners/Components

| Products | | Technology Partners | Notes |
|---|---|---|---|
| **Rack Workstation** | | | |
| | CoreStation WR3930 | Dell EMC Precision 3930, 7920, BIOS, Intel Xeon/Core CPUs. Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s), Apps[1] | See vendor guidance below |
| | CoreStation WR7920 | | See vendor guidance below. Tera2 not vulnerable - see notes below. |

[1] Such as Teradici Management Console, PCoIP Connection Manager, VMware Horizon (broker), Leostream Broker/Gateway

| Products | | Technology Partners | Notes |
|---|---|---|---|
| **Blade Workstation** | | | |
| | CoreStation MX740c | Dell EMC PE MX740c server, iDRAC, BIOS. Client OS: Windows / Linux. Apps: Teradici Cloud Access Software (CAS), NVIDIA License Server, NVIDIA GRID, Leostream Broker/Gateway | See vendor guidance below<br>Per Dell, PE BIOS not vulnerable. |
| | MX7000 system components | Dell EMC PE MX7000 enclosure components such as fabric switches, MM, OME-Modular etc. | See vendor guidance below. |
| | CoreStation WFC640 | Dell EMC PE FC-series server, iDRAC, BIOS, Intel Xeon CPUs, Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s), Apps[1] | See vendor guidance below.<br>Tera2 not vulnerable - see notes below. |
| | FX2 system components | Dell EMC PE FX2 enclosure components such as switches, CMC etc. | See vendor guidance below. Per Dell, PE CMC not vulnerable. |
| | CoreStation WM640 | Dell EMC PE M-series server, iDRAC, Dell customized BIOS, Intel Xeon CPUs, Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s), Apps[1] | *See vendor guidance below.*<br>*Per Dell, PE BIOS not vulnerable. Tera2 not vulnerable - see notes below.* |
| | CoreStation DXM630 | | See vendor guidance below.<br>Per *Dell, PE BIOS not vulnerable.*<br>Tera2 not vulnerable - see notes below. |
| | CoreStation DXM620, DXM520, DXM420 | | See vendor guidance below.<br>Per *Dell, PE BIOS not vulnerable*. Tera2 not vulnerable - see notes below. |
| | CoreStation DXM710, DXM610 | | See vendor guidance below.<br>Per *Dell, PE BIOS not vulnerable.* Tera2 not vulnerable - see notes below. |
| | M1000e system components | Dell EMC PE M1000e enclosure components such as blade interconnect, CMC etc. | See vendor guidance below. Per Dell, PE CMC not vulnerable. |

| Products | | Technology Partners | Notes |
|---|---|---|---|
| **Virtual Blade Workstation / Virtual Desktop Servers** | | | |
| | CoreStation MX740c | Dell EMC PE MX740c server, iDRAC, BIOS, VMware vSphere, Horizon, NVIDIA License Server, NVIDIA GRID, Teradici CAS | See vendor guidance below.<br>Per *Dell, PE BIOS not vulnerable.* |
| | CoreStation VM640 | Dell EMC PE M640 or M630 server, iDRAC, BIOS, Intel Xeon CPUs, VMware vSphere, Horizon, NVIDIA License Server, NVIDIA GRID, Teradici CAS | See vendor guidance below.<br>Per *Dell, PE BIOS not vulnerable.* |
| | CoreStation VM630 | | See vendor guidance below.<br>Per *Dell, PE BIOS not vulnerable.* |
| | CoreStation VFC640 | Dell EMC PE FX2 server, iDRAC, BIOS, Intel Xeon CPUs, VMware vSphere, Horizon, NVIDIA License Server, NVIDIA GRID, Teradici CAS | See vendor guidance below<br>Per *Dell, PE BIOS not vulnerable.* |
| | MX7000, FX2s and M1000e system components | Dell EMC PE MX7000, FX2s or M1000e enclosure components such as blade interconnect, CMC etc. | See vendor guidance below. Per Dell, PE CMC not vulnerable. |

| Products | | Technology Partners | Notes |
|---|---|---|---|
| **KVM Extender and Remote Workstation Graphics Cards** | | | |
| | DMX, DXP4 | Teradici Tera2 PCoIP processor, ARM 'BSM' processor, NVIDIA GPU. | See vendor guidance below. Tera2 not vulnerable - see notes below. |
| **KVM Extender and Remote Workstation Cards** | | | |
| | DXH, DXL | Teradici Tera2 PCoIP processor, ARM 'BSM' processor. Apps[2] | Not vulnerable - see notes below. |
| | DXR-H4, DXT-H4 | Teradici Tera2 PCoIP processor, Intel Atom, Win10 IoT OS, ARM 'BSM' processor, VMware Horizon Agent. Apps[2] | Tera2 not vulnerable. Per Intel guidance the Atom model is not affected. |
| **DXZ Zero Clients** | | | |
| | DXZ models, DXR-Z4 | Teradici Tera2 PCoIP processor, ARM 'BSM' processor. Apps[2] | Not vulnerable - see notes below. |
| **DX Thin Clients** | | | |
| | DX3240 models | Dell Precision BIOS, Intel Core processor, Stratodesk NTOS, NoTouch Center, Teradici CAS | See vendor guidance below. |
| **KM Switches** | | | |
| | K4u+ | Amulet Hotkey firmware for custom FPGAs, MousePoint software | Not vulnerable - see notes below. |

Table 2: Vendor Guidance Links:

| Vendor | Advisory Type | Link |
|---|---|---|
| Apache.org | Security Advisory | https://logging.apache.org/log4j/2.x/security.html |
| | Blog | https://lists.apache.org/thread/0x4zvtq92yggdgvwfgsftqrj4xx5w0nx |
| Citrix | Security Advisory | https://discussions.citrix.com/topic/415000-citrix-products-affected-from-log4j-zero-day-vulnerability-cve-2021-44248/ |
| | Blog | https://www.citrix.com/blogs/2021/12/13/guidance-for-reducing-apache-log4j-security-vulnerability-risk-with-citrix-waf/ |
| Dell EMC | Security Advisory | https://www.dell.com/support/security/en-gy |
| | KB article | Products impacted: https://www.dell.com/support/kbdoc/000194414 |
| | KB article | https://www.dell.com/support/kbdoc/en-ca/000194372/dsn-2021-007-dell-response-to-apache-log4j-remote-code-execution-vulnerability |
| | KB article | https://www.dell.com/support/kbdoc/en-gy/000194416/additional-information-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228 |
| HP/Teradici | KB article | https://support.hp.com/us-en/document/ish_5268006 |
| Microsoft | Security Guidance | https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013 |
| | Security Advisory | https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/ |
| Leostream | KB article | https://support.leostream.com/support/discussions/topics/66000507567 |
| NVIDIA | Security Advisory | https://www.nvidia.com/en-us/security/<br>https://nvidia.custhelp.com/app/answers/detail/a_id/5294 |
| | KB article | https://enterprise-support.nvidia.com/s/article/Log4j-Java-Vulnerability-CVE-2021-44228-for-vGPU-Legacy-License-Server |
| RedHat | Security Advisory | https://access.redhat.com/security/cve/cve-2021-44228<br>https://access.redhat.com/security/cve/CVE-2021-4104<br>https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-17571<br>https://access.redhat.com/security/vulnerabilities/RHSB-2021-009 |
| Stratodesk | KB article | https://www.stratodesk.com/kb/Main_Page |
| SuSe | Security Advisory | https://www.suse.com/c/suse-statement-on-log4j-log4shell-cve-2021-44228-vulnerability/<br>https://www.suse.com/security/cve/CVE-2021-44228.html |
| | KB article | https://www.suse.com/support/kb/doc/?id=000020526 |
| Ubuntu | Security Advisory | https://ubuntu.com/security/notices/USN-5192-1<br>https://ubuntu.com/security/CVE-2021-44228 |
| | Security Advisory | https://ubuntu.com/security/notices/USN-4495-1 |
| VMware | Security Advisory | https://www.vmware.com/security/advisories/VMSA-2021-0028.html |
| | KB article | Horizon: https://kb.vmware.com/s/article/87073 |

| | | |
|---|---|---|
| | | UAG: https://kb.vmware.com/s/article/87092 |

**Amulet Hotkey Zero Clients and Host Cards**

Amulet Hotkey zero client and KVM Extender/Remote Workstation products incorporate Teradici Tera2 PCoIP processors and ARM 'BSM' processors. The BSM is not affected as it does not have an OS and no web interface, Apache or Log4j. Teradici have confirmed that the Tera2 processors are not vulnerable.

- Tera2 Processor firmware does not permit the installation or execution of user applications.
- Teradici controls the firmware and a digital signature must be present for the Tera2 to allow a firmware installation (upgrade or downgrade of firmware).

***Important note:*** *while Tera2 zero clients and remote workstation cards are not directly vulnerable, they may be used to connect to host systems, workstations or virtual desktops that may be vulnerable. Those host systems must be protected accordingly.*

**Amulet Hotkey DXR-H4 / DXT-H4 KVM Extender Hosts**

Amulet Hotkey DXR-H4 and DXT-H4 KVM extender host cards incorporate Teradici Tera2 PCoIP processor, Intel Atom processor, and ARM 'BSM' processors, Windows 10 IoT operating system and VMware Horizon Agent. The Tera2 processor is not vulnerable (see below). There is no LDAP support and all authentication is local windows based. There is no web interface, Apache or Log4j. The BSM is not affected as it does not have an OS or network interface. The VMware Horizon Agent 7.12 that is packaged with Amulet Hotkey firmware 1.14 is not vulnerable.

***Note:*** *while VMware Horizon Agent 7.13.x is only vulnerable only vRealize Operations feature is installed, this feature is not installed by default.*

**Amulet Hotkey K4u+ KM Switch**

Amulet Hotkey K4u+ is not affected as it does not have an OS or network connection.

**Change History:**

| Date | Change |
|---|---|
| 12/15/2021 | Notice published |
| 12/16/2021 | Added CVE-2021-45046, CVE-2020-9488, CVE-2017-5645. Updated Table 1 notes. |
| | |
| | |



If you have questions about this notice, please contact Amulet Hotkey.

Amulet Hotkey | London, +44 (0) 20 7960 2400 | New York, +1 212-269-9300
www.amulethotkey.com | sales@amulethotkey.com