AMULET HOTKEY

Advisory Notice

OpenSSL vulnerabilities and impact on Amulet Hotkey products

Summary

April 28, 2022

New security vulnerabilities have been disclosed. 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. See vendor guidance below which may list additional vulnerabilities.

Contents

Vulnerabilities

Expat library	Potential integer overflow errors		
Mechanism for triggering	Potential integer overflow errors		
Affected platforms	Integer overflow and invalid shift that could lead to uncontrollable resources consumption, elevation of privileges and remote control execution.		
Systems affected	Any system using open source Expat Library software version before 2.4.3.		
Difficulty of successful attack	CVE ID	Score, Severity	CVSS Vector
	CVE-2022-22824	9.8 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	CVE-2022-22823	9.8 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	CVE-2022-22822	9.8 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	CVE-2022-22827	8.8 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
	CVE-2022-22826	8.8 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
	CVE-2022-22825	8.8 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
	CVE-2021-45960	8.8 High	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	CVE-2021-46143	8.1 High	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

OpenSSL	Denial of service from infinite loop (CVE-2022-0778) and carry propagation bug (CVE-2021-4160)		
Mechanism for triggering	Potential infinite loop when parsing certificates containing elliptic curve public keys that results in denial of service. Carry propagation bug in MIPS32/MIPS64 squaring procedure that can affect handling certificates containing elliptic curve keys, including some TLS1.3 default curves.		
Affected platforms	Any system using OpenSSL versions 1.0.2 (EOL), 1.1.1 and 3.0 (CVE-2022-0778) and OpenSSL versions 1.0.2 (EOL), 1.1.1 and 3.0 on MIPS platforms (CVE-2021-4160)		
Systems affected	Systems/applications processing certificates containing elliptic curve keys including Teradici		
Difficulty of successful attack	CVE ID	Score, Severity	CVSS Vector
	CVE-2022-0778	7.5 High	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
	CVE-2021-4160	5.9 Medium	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

<table>
<tr><th>Mongoose</th><th>Files and directories accessible</th></tr>
<tr><td>Mechanism for triggering</td><td>Unsafe handling of file names during upload may enable files to be written to arbitrary locations outside of the target folder.</td></tr>
<tr><td>Affected platforms</td><td>Any system using the cesanta/mongoose package before version 7.6</td></tr>
<tr><td>Systems affected</td><td>Systems applications with Mongoose web server including Teradici Cloud Access Software</td></tr>
<tr><td>Difficulty of successful attack</td><td>
<table>
<tr><th>CVE ID</th><th>Score, Severity</th><th>CVSS Vector</th></tr>
<tr><td>CVE-2022-25299</td><td>7.5 High</td><td>CVSS:CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Tianocore EDK2</th><th>Authentication bypass and buffer overflow</th></tr>
<tr><td>Mechanism for triggering</td><td>Null pointer dereference in EDK2 may allow an authenticated user to enable escalation of privilege. Heap overflow in LzmaUefiDecompressGetInfo, unlimited recursion in DxeCore in EDK2</td></tr>
<tr><td>Affected platforms</td><td>Any system using the Tianocore EDK2</td></tr>
<tr><td>Systems affected</td><td>System BIOS using Tianocore EDK2 including Dell PowerEdge</td></tr>
<tr><td>Difficulty of successful attack</td><td>
<table>
<tr><th>CVE ID</th><th>Score, Severity</th><th>CVSS Vector</th></tr>
<tr><td>CVE-2021-28210</td><td>7.8 High</td><td>CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</td></tr>
<tr><td>CVE-2019-14584</td><td>7.8 High</td><td>CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</td></tr>
<tr><td>CVE-2021-28211</td><td>6.7 Medium</td><td>CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</td></tr>
</table>
</td></tr>
</table>

Amulet Hotkey Products and Solution Partners/Components

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

- **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. We recommend that you monitor critical systems accordingly.

Important Notes for the Product Tables

[1] - See the latest information from the applicable vendor in the Vendor Guidance Links section.

[2] - See the Amulet Hotkey Products – Additional Notes section.

Rack Workstation

Products	Technology Partners	Notes[1]
CoreStation WR3930	Dell EMC Precision 3930, 7920, BIOS, Intel Xeon/Core CPUs. Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s)	Tera2 host not vulnerable[2].
CoreStation 7920r		

Blade Workstation

Products	Technology Partners	NotesError! Bookmark not defined.
CoreStation MX750c	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	Check Dell BIOS and Teradici update guidance[1]
CoreStation MX740c		
MX7000 system components	Dell EMC PE MX7000 enclosure components such as fabric switches, MM, OME-Modular etc.	See Note[1]
CoreStation WFC640, WFC630	Dell EMC PE FC-series server, iDRAC, BIOS, Intel Xeon CPUs, Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s)	Check Dell BIOS update guidance[1] Tera2 host not vulnerable[2]
FX2 system components	Dell EMC PE FX2 enclosure components such as switches, CMC etc.	See Note[1]
CoreStation WM640	Dell EMC PE M-series server, iDRAC, Dell customized BIOS, Intel Xeon CPUs, Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s)	Check Dell BIOS update guidance[1] Tera2 host not vulnerable[2]
CoreStation DXM630		
CoreStation DXM620, DXM520, DXM420		See Note[1] Tera2 host not vulnerable[2]
CoreStation DXM710, DXM610		
M1000e system components	Dell EMC PE M1000e enclosure components: blade interconnect, CMC etc.	See Note[1]

Virtual Blade Workstation / Virtual Desktop Servers

Products	Technology Partners	Notes
CoreStation MX750c	Dell EMC PE MX740c server, iDRAC, BIOS, VMware vSphere, Horizon, NVIDIA License Server, NVIDIA GRID, Teradici CAS	Check Dell BIOS and Teradici update guidance[1]
CoreStation MX740c		
CoreStation VM640	Dell EMC PE M-series server, iDRAC, BIOS, Intel Xeon CPUs, VMware vSphere, Horizon, NVIDIA License Server, NVIDIA GRID, Teradici CAS	
CoreStation VM630		
CoreStation VFC640	Dell EMC PE FX2 server, iDRAC, BIOS, Intel Xeon CPUs, VMware vSphere, Horizon, NVIDIA License Server, NVIDIA GRID, Teradici CAS	
CoreStation VFC630		
MX7000, FX2s and M1000e system components	Dell EMC PE MX7000, FX2s or M1000e enclosure components such as blade interconnect, CMC etc.	See Note[1]

KVM Extender and Remote Workstation Graphics Cards

Products	Technology Partners	Notes
DMX, DXP4	Teradici Tera2 PCoIP processor, ARM 'BSM' processor, NVIDIA GPU	See Note[1] Tera2 host not vulnerable[2]

KVM Extender and Remote Workstation Cards

Products	Technology Partners	Notes
DXH, DXL	Teradici Tera2 PCoIP processor, ARM 'BSM' processor. Apps	See Note[1] Tera2 host not vulnerable[2]
DXR-H4, DXT-H4	Teradici Tera2 PCoIP processor, Intel Atom, Win10 IoT OS, ARM 'BSM' processor, VMware Horizon Agent. Apps	

DXZ Zero Clients

Products	Technology Partners	Notes
DXZ models, DXR-Z4	Teradici Tera2 PCoIP processor, ARM 'BSM' processor. Apps	See Note[1].Check Teradici firmware update guidance.

DX Thin Clients

Products	Technology Partners	Notes
DX3240 models	Dell Precision BIOS, Intel Core processor, Stratodesk NTOS, NTC, Teradici CAS	See Note[1] Stratodesk NTOS 3.3.727 uses Teradici CAS Client 22.01.3.

KM Switches

Products	Technology Partners	Notes
K4u+	Amulet Hotkey firmware for custom FPGAs, MousePoint software	Not vulnerable[2]

Vendor Guidance Links

Vendor	Advisory Type	Link
HP/Teradici	Security Advisory	https://support.hp.com/us-en/security-bulletins
OpenSSL	Security Advisory	https://www.openssl.org/news/secadv/20220315.txt https://www.openssl.org/news/secadv/20220128.txt
Dell EMC	Security Advisory	https://www.dell.com/support/security/en-us
NVIDIA	KB article	https://www.dell.com/support/kbdoc/en-ca/000198065/dsa-2022-088
Stratodesk	Security page	https://www.nvidia.com/en-us/security/
VMware	KB article	https://www.stratodesk.com/kb/Main_Page

Amulet Hotkey Products – Additional Notes

Amulet Hotkey Host Cards

Amulet Hotkey KVM Extender/Remote Workstation hosts and PCIe card 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. Teradici have confirmed that the Tera2 host 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 remote workstation hosts/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 host processor is not vulnerable. The BSM is not affected as it does not have an OS or network interface.

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
5/11/2022	Notice published

The information provided in this notice is believed to be accurate and reliable as of the date provided. However, Amulet Hotkey Ltd does not give any representations or warranties, expressed or implied as to the accuracy or completeness of such information. Amulet Hotkey shall have no liability of the consequences or use of such information for any infringement of other rights from third parties that may result from its use.

Amulet Hotkey reserves the right to make corrections modifications and other changes to this notice at any time. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

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

Resources
https://resources.amulethotkey.com/resources

EMEA Support
+44(0)20 7960 2400
eurosupport@amulethotkey.com

North America Support
+1(212)269 9300
ussupport@amulethotkey.com
casupport@amulethotkey.com

Asia Pacific Support
apsupport@amulethotkey.com

Latin America Support
latamsupport@amulethotkey.com