MONTELEKTRO

SJEDIŠTE RIJEKA
Kudeji 53
HR-51215 Kastav
rijeka@montelektro.hr
+ 385 51 54 58 10

URED ZAGREB
Marka Marulića 5
HR-10431 Sv. Nedelja
zagreb@montelektro.hr
+ 385 1 39 09 020

Security Advisory

CVE-2021-44228 Apache Log4j

Revision history:

Date	Rev.	Description
20.12.2021.	2	Added additional relevant vendors: Cisco, HPE, LogMeIn, NAKIVO, QNAP, Schneider Electric, TeamViewer
16.12.2021.	1	Initial release

MONTELEKTRO

TABLE OF CONTENTS

1. INTRODUCTION

A critical vulnerability in Apache Log4j identified by CVE-2021-44228 and a low severity vulnerability identified by CVE-2021-45046 have been publicly disclosed. This vulnerability allows for remote code execution by exploiting the Java Logging Library log4j2. Montelektro is aware of this vulnerability and of how it could, if exploited, potentially impact our customers' environments.

Montelektro is continuously monitoring security advisories published by vendors of the components that are used in our IT infra and PCS solutions.

This is an ongoing event, please check this advisory for frequent updates as they develop.

2. MONITORED PRODUCTS

Vulnerability exposure status of Montelektro PCS relevant products confirmed by their vendors.

2.1. AFFECTED PRODUCTS

Table 1 - Products affected and confirmed by the vendor

Vendor	Product	Security advisory
HPE	3PAR Service Processor (versions 5.x)	HPE Security bulletin - HPESBGN04215 rev.5 - Certain HPE Products using Apache Log4j2, Remote Arbitrary Code Execution – December 18, 2021
	Intelligent Management Center (E0706 P06)	HPE Support alert - HPE Intelligent Management Center - Security Advisory for Apache Log4j2 Vulnerability (CVE-2021-44228) – December 17, 2021
	SimpliVity 325 (versions 4.1.1, 4.1.0U1, 4.1.0, 4.0.1U1, 4.0.1, 4.0.0, 3.7.10U1, 3.7.10/3.7.10A, 3.7.9)	HPE Security bulletin - HPESBGN04215 rev.5 - Certain HPE Products using Apache Log4j2, Remote Arbitrary Code Execution – December 18, 2021
	SimpliVity OmniCube (versions 3.7.10/3.7.10A, 3.7.9)	HPE Security bulletin - HPESBGN04215 rev.5 - Certain HPE Products using Apache Log4j2, Remote Arbitrary Code Execution – December 18, 2021
	StoreServ Management Console (SSMC) versions prior to v3.8.2.1	HPE Security bulletin - HPESBGN04218 rev.1 - HPE 3PAR/Primera StoreServ Management Console (SSMC), Apache Log4j 2 Remote Arbitrary Code Execution – December 18, 2021
NAKIVO	NAKIVO Backup & Replication versions prior to v10.5.1	NAKIVO Knowledge base - Log4j2 (CVE-2021-44228) Vulnerability – December 15, 2021
Proficy / GE	Proficy Historian with Web Components (version 9.1)	GE Digital Plant Manufacturing and Proficy Product Security Communication - December 15, 2021
Schneider Electric	APC PowerChute Business Edition (versions 9.5, 10.0, 10.0.1, 10.0.2, 10.0.3, 10.0.4) APC PowerChute Network Shutdown (versions 4.4.1, 4.4, 4.3, 4.2)	Schneider Electric Security Notification - Apache Log4j Vulnerability (Log4Shell) v4.0 – December 17, 2021
VMware	vCenter Server 7.x, 6.7.x, 6.5.x virtual appliance vCenter Server 6.7.x, 6.5.x Windows	VMware Security Advisory VMSA-2021-0028.3 - Updated On 2021-12-15

2.2. UNAFFECTED PRODUCTS

Table 2 - Not affected products confirmed by the vendor

Vendor	Product	Security advisory
Cisco	Entire relevant portfolio	Cisco Security advisory - Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021 v1.23 – December 19, 2021
ESET	Entire relevant portfolio	[ALERT8188] Information regarding the Log4j 2 vulnerability
HPE	Aruba networking relevant portfolio	HPE Security bulletin - HPESBNW04216 rev.1 - HPE Aruba Silver Peak Orchestrator, Remote Arbitrary Code Execution – December 16, 2021
LogMeIn	Hamachi	LogMeIn's Response to Log4j – Remediated – publish date not specified
Microsoft	Entire relevant portfolio	Microsoft's Response to CVE-2021-44228 Apache Log4j 2 2021 Dec 11, updated 2021 Dec 15.
Proficy / GE	iFIX HMI/SCADA Webspace Licensing Historian (versions 6.0, 7.0, 7.1, 7.2, 8.0, 8.1, 9.0), Historian 9.1 *(when the web components have been excluded from the install)* Industrial Gateway Server, Win 911	GE Digital Plant Manufacturing and Proficy Product Security Communication - December 15, 2021
ProLeiT	Entire portfolio	Critical vulnerability in JAVA library Log4j - (CVE-2021-44228) - Press News 12/15/2021
Qlik	Entire relevant portfolio	Qlik Vulnerability Testing - Apache Log4j, reference CVE-2021-44228 (also referred to as Log4Shell)
QNAP	Entire relevant portfolio	QNAP Security advisory Vulnerability in Apache Log4j Library v1.1 – December 15, 2021
Rockwell	Entire relevant portfolio	Rockwell Log4Shell Vulnerability Notice - Version 1.1, 15-Dec-2021. Updated Affected Products and Risk Mitigation & User Actions
Secomea	Entire portfolio	Other security statements - Statement on Log4Shell vulnerability – CVE-2021-44228
Siemens	Entire relevant portfolio	SSA-661247: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to Siemens Products v1.2
TeamViewer	Entire portfolio (server-side patch deployed)	TeamViewer Security bulletins - Server-side hotfix for log4J issue, December 15, 2021
VMware	vSphere ESXi Workstation Workstation Player Tools	VMware Response to CVE-2021-44228: Apache Log4j Remote Code Execution (87068) - Updated On 2021-12-15

3. CURRENTLY AVAILABLE MITIGATIONS

3.1. HPE - 3PAR SERVICE PROCESSOR (VERSIONS 5.X)

Patch release pending.

No workaround available at the moment.

3.2. HPE - INTELLIGENT MANAGEMENT CENTER (E0706 P06)

Patch release pending.

Workaround available: HPE Support alert - HPE Intelligent Management Center - Security Advisory for Apache Log4j2 Vulnerability (CVE-2021-44228) – December 17, 2021, chapter Details.

3.3. HPE - SIMPLIVITY 325 (4.1.1, 4.1.0U1, 4.1.0, 4.0.1U1, 4.0.1, 4.0.0, 3.7.10U1, 3.7.10/3.7.10A, 3.7.9)

Patch release pending.

No workaround available at the moment.

3.4. HPE - SIMPLIVITY OMNICUBE (VERSIONS 3.7.10/3.7.10A, 3.7.9)

Patch release pending.

No workaround available at the moment.

3.5. HPE - STORESERV MANAGEMENT CONSOLE (SSMC) VERSIONS PRIOR TO V3.8.2.1

Patch released in v3.8.2.1.

3.6. NAKIVO - BACKUP & REPLICATION VERSIONS PRIOR TO V10.5.1

Patch released in v10.5.1.

Manual fix instructions available: NAKIVO Knowledge base article Log4j2 (CVE-2021-44228) Vulnerability, chapter Manual Fix.

3.7. PROFICY / GE - PROFICY HISTORIAN WITH WEB COMPONENTS (V9.1)

Patch release pending.

Workaround available: GE Digital Plant Manufacturing and Proficy Product Security Communication - December 15, 2021 – Chapter Recommended Mitigations.

3.8. SCHNEIDER ELECTRIC - APC POWERCHUTE BUSINESS EDITION (VERSIONS 9.5, 10.0, 10.0.1, 10.0.2, 10.0.3, 10.0.4)

Patch release pending.

Workaround available: Schneider Electric Security Notification - Apache Log4j Vulnerability (Log4Shell) v4.0 – December 17, 2021 – Table Affected Products, column Recommended Mitigation.

3.9. SCHNEIDER ELECTRIC - APC POWERCHUTE NETWORK SHUTDOWN (VERSIONS 4.4.1, 4.4, 4.3, 4.2)

Patch release pending.

Workaround available: Schneider Electric Security Notification - Apache Log4j Vulnerability (Log4Shell) v4.0 – December 17, 2021 – Table Affected Products, column Recommended Mitigation.

3.10. VMWARE - VCENTER SERVER 7.X, 6.7.X, 6.5.X VIRTUAL APPLIANCE

Patch release pending.

Workaround available: VMware Workaround instructions to address CVE-2021-44228 in vCenter Server and vCenter Cloud Gateway (87081).

3.11. VMWARE - VCENTER SERVER 6.7.X, 6.5.X WINDOWS

Patch release pending.

Workaround available: VMware Workaround instructions to address CVE-2021-44228 in vCenter Server Windows (87096).

4. MITIGATION RECOMMENDATIONS

As a general security measure, Montelektro strongly recommends protecting network access to devices with appropriate mechanisms.

Workaround deployment on affected systems which are not exposed to the outside world should be postponed until final patch is released by the vendor.

Patch planning and administration guidelines from Montelektro PCS IT maintenance and security whitepaper should be considered during the patch deployment.

An active SLA contract can be used to support the installation of the patch on components supplied by Montelektro.

MONTELEKTRO

5. REFERENCES

Cisco. (2021, December 19). *Cisco Security advisory - Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021 v1.23.* Retrieved from Cisco Security Advisories: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

ESET. (2021, December 15). *[ALERT8188] Information regarding the Log4j 2 vulnerability*. Retrieved from https://support.eset.com/en/alert8188-information-regarding-the-log4j2-vulnerability

GE. (2021, December 15). *GE Digital Plant Manufacturing and Proficy Product Security Communication*. Retrieved from https://digitalsupport.ge.com/en_US/Article/GE-Digital-Plant-Manufacturing-Log4j-Product-Communication-GED-21-02

HPE. (2021, December 17). *HPE Support alert - HPE Intelligent Management Center - Security Advisory for Apache Log4j2 Vulnerability (CVE-2021-44228).* Retrieved from HPE Support center: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00120130en_us

HPE. (2021, December 18). *HPESBGN04215 rev.5 - Certain HPE Products using Apache Log4j2, Remote Arbitrary Code Execution.* Retrieved from HPE Support center: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04215en_us

HPE. (2021, December 18). *HPESBGN04218 rev.1 - HPE 3PAR/Primera StoreServ Management Console (SSMC), Apache Log4j 2 Remote Arbitrary Code Execution.* Retrieved from HPE Support center: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04218en_us

HPE. (2021, December 16). *HPESBNW04216 rev.1 - HPE Aruba Silver Peak Orchestrator, Remote Arbitrary Code Execution.* Retrieved from HPE Support center: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04216en_us

LogMeIn. (2021, December). *LogMeIn's Response to Log4j — Remediated.* Retrieved from Support portal: https://support.logmeininc.com/pro/help/logmeins-response-to-log4j

Microsoft. (2021, December 15). *Microsoft's Response to CVE-2021-44228 Apache Log4j*. Retrieved from https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

Montelektro. (2019, July). *Process Control System – IT maintenance and security Whitepaper.* Retrieved from https://www.montelektro.hr/wp-content/uploads/2021/12/White-paper-PCS-IT-maintenance-and-security-R01.pdf

NAKIVO. (2021, December 15). *Log4j2 (CVE-2021-44228) Vulnerability.* Retrieved from Knowledge Base: https://helpcenter.nakivo.com/display/KB/Log4j2+%28CVE-2021-44228%29+Vulnerability

NIST. (2021, December 16). *CVE-2021-44228 Detail*. Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

ProLeiT. (2021, December 15). *Critical vulnerability in JAVA library Log4j - (CVE-2021-44228) - Press News*. Retrieved from https://www.proleit.com/news-events/press/?tx_news_pi1%5Bnews%5D=349&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=8a167e2c359107f1a6d16749b55114f3

Qlik. (2021, December 15). *Vulnerability Testing - Apache Log4j, reference CVE-2021-44228 (also referred to as Log4Shell)*. Retrieved from https://community.qlik.com/t5/Support-Updates-Blog/Vulnerability-Testing-Apache-Log4j-reference-CVE-2021-44228-also/ba-p/1869368

QNAP. (2021, December 15). *Vulnerability in Apache Log4j Library.* Retrieved from QNAP Security Advisories: https://www.qnap.com/en/security-advisory/qsa-21-58

Rockwell. (2021, December 15). *Rockwell Log4Shell Vulnerability Notice - Version 1.1*. Retrieved from https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1133605

Schneider Electric. (2021, December 17). *Security Notification - Apache Log4j Vulnerability (Log4Shell).* Retrieved from https://www.se.com/ww/en/download/document/SESB-2021-347-01/

Secomea. (2021, December 13). *Other security statements - Statement on Log4Shell vulnerability – CVE-2021-44228.* Retrieved from https://www.secomea.com/support/cybersecurity-advisory/

Siemens. (2021, December 16). *SSA-661247: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to Siemens Products v1.2*. Retrieved from https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf

TeamViewer. (2021, December 15). *Security bulletins - Server-side hotfix for log4J issue.* Retrieved from Trust Center: https://www.teamviewer.com/en/trust-center/security-bulletins/hotfix-log4j2-issue/?_ga=2.206685072.242790736.1639989472-1764969916.1639989472

VMware. (2021, December 15). *VMware Response to CVE-2021-44228: Apache Log4j Remote Code Execution (87068)*. Retrieved from https://kb.vmware.com/s/article/87068

VMware. (2021, December 15). *VMware Security Advisory VMSA-2021-0028.3*. Retrieved from https://www.vmware.com/security/advisories/VMSA-2021-0028.html

VMware. (2021, December 16). *VMware Workaround instructions to address CVE-2021-44228 in vCenter Server and vCenter Cloud Gateway (87081)*. Retrieved from https://kb.vmware.com/s/article/87081?lang=en_US

VMware. (2021, December 15). *VMware Workaround instructions to address CVE-2021-44228 in vCenter Server Windows (87096)*. Retrieved from https://kb.vmware.com/s/article/87096