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
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
Proficy / GE	Proficy Historian with Web Components (version 9.1)	GE Digital Plant Manufacturing and Proficy Product Security Communication - December 15, 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
ESET	Entire relevant portfolio	[ALERT8188] Information regarding the Log4j 2 vulnerability
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)
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
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. PROFICY / GE-PROFICY HISTORIAN WITH WEB COMPONENTS (VERSION 9.1)

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

3.2. 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).

3.3. 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.

5. REFERENCES

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

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

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

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

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

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