SSA-661247: Apache Log4j Vulnerability (CVE-2021-44228, Log4Shell) - Impact to Siemens Products

Publication Date: 2021-12-13
Last Update: 2021-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

On 2021-12-09, a vulnerability in Apache Log4j (a logging tool used in many Java-based applications) was disclosed, that could allow remote unauthenticated attackers to execute code on vulnerable systems. The vulnerability is tracked as CVE-2021-44228 and is also known as “Log4Shell”.

Siemens is currently investigating to determine which products are affected and is continuously updating this advisory as more information becomes available. See section Additional Information for more details regarding the investigation status.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
E-Car OC Cloud Application: All versions < 2021-12-13	Vulnerability fixed on central cloud service starting 2021-12-13; no user actions necessary See further recommendations from section Workarounds and Mitigations
EnergyIP Prepay: V3.7, V3.8	Specific mitigation information has been released for the customer projects with the request of immediate deployment. The long-term solution of updating the log4j2 component to version 2.15 is being tested and will be released, once confirmed being safe for the particular product version in line with the project Service Level Agreements. See further recommendations from section Workarounds and Mitigations
Industrial Edge Management App (IEM-App): All versions	Exposure to vulnerability is limited as IEM-App runs in IEM-OS and IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview https://support.industry.siemens.com/cs/us/en/view/109804061 See further recommendations from section Workarounds and Mitigations
Industrial Edge Management OS (IEM-OS): All versions	Exposure to vulnerability is limited as IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview: https://support.industry.siemens.com/cs/us/en/view/109804061 See further recommendations from section Workarounds and Mitigations

Industrial Edge Manangement Hub: All versions	Vulnerability fixed on central cloud service starting 2021-12-13; no user actions necessary See further recommendations from section Workarounds and Mitigations
LOGO! Soft Comfort: All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
Mendix Applications: All versions	Although the Mendix runtime itself is not vulnerable to this exploit, we nevertheless recommend to upgrade log4j-core to at least version 2.15.0 in case log4j-core is part of your project. This advice is regardless of the JRE/JDK version the app runs on. https://status.mendix.com/incidents/8j5043my610c See further recommendations from section Workarounds and Mitigations
Mindsphere Cloud Application: All versions < 2021-12-11	Vulnerability fixed on central cloud service starting 2021-12-11; no user actions necessary See further recommendations from section Workarounds and Mitigations
Operation Scheduler: All versions >= V1.1.3	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
SIGUARD DSA: V4.2, V4.3, V4.4	Adapt the client and computation node start-up batch scripts or shell scripts by adding -Dlog4j2.formatMsgNoLookups=true directly after the java statement. Adapt the application server start-up by adding -Dlog4j2.formatMsgNoLookups=true somewhere after the standalone.sh statement. Stop and restart the SIGUARD DSA processes. See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.4: All versions < V7.4 SP1	Update to V7.4 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109746038 Only connect to trusted OPC UA servers See further recommendations from section Workarounds and Mitigations
Siveillance Command: All versions >= 4.16.2.1	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations

Siveillance Control Pro: All versions	Hotfix available for versions >= V2.1 (please contact customer support) Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations
Siveillance Vantage: All versions	Currently no remediation is available Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- If the specific Siemens product (which is currently using Log4j versions >= 2.10 and < 2.15.0 in its versions released so far) allows it: Set the parameter log4j2.formatMsgNoLookups to 'true'. The two most common options to set this parameter in the Java Virtual Machine are: as cmdline parameter ('-Dlog4j2.formatMsgNoLookups=true') or as environment variable ('LOG4J_FORMAT_MSG_NO_LOOKUPS="true"').
- If the specific Siemens product (which is currently using Log4j versions 2.0-beta9 to 2.10.0 in its versions released so far) allows it: Remove the JndiLookup class from the classpath: 'zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class'
- If the specific Siemens product (which is currently using Log4j versions >=2.7 and <2.15.0 in its versions released so far) allows it: Modify all PatternLayout patterns to specify the message converter as '%m{nolookups}' instead of just '%m'.
- If the specific Siemens product allows it: Update the Log4j component to 2.15.0 or later versions on the systems where the product is installed.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

E-Car OC (E-Car Operation Center) is a cloud service that manages charging infrastructures for electric vehicles (EVs), both in domestic and public or semi-public areas.

EnergyIP applications enable utilities, retailers, DSO's and market operators proven technology to meet the needs and requirements of the energy sector.

EnergyIP Prepay is an end-to-end solution for smart prepaid energy management. It features flexible tariff management, real-time rating and charging, convenient payment, and recharging options as well as intelligent energy consumption control features.

Geolus software is a geometry-based search engine for both single and multi-CAD environment PLM stakeholders who need to reduce/control part costs throughout the product lifecycle, manage engineering design knowledge and increase manufacturing efficiencies.

HES UDIS (Head-End System Universal Device Integration System) is an integrated solution for processing meter data and device events.

Industrial Edge Management (IEM) enables a centralized management of Siemens Industrial Edge Devices and Edge Applications. IEM is tailored to customer's needs and is operated by the customer (on-premises).

LOGO! Soft Comfort is an engineering software to configure and program LOGO! BM (Base Module) devices.

Mendix is a high productivity app platform that enables you to build and continuously improve mobile and web applications at scale. The Mendix Platform is designed to accelerate enterprise app delivery across your entire application development lifecycle, from ideation to deployment and operations.

MindSphere is an industrial IoT as a service solution.

Operation Scheduler is a tool that enables security operators to intelligently perform routine tasks. It can be used to schedule maintenance tasks.

SIGUARD DSA is a model-based dynamic stability assessment tool for online control room use and offline operational planning purposes.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SiPass integrated is a powerful and extremely flexible access control system.

Siveillance Control Pro is a command and control solution, specifically designed to support security management at critical infrastructure sites such as ports, airports, oil and gas power generation and distribution, chemical and pharma industries, heavy industries and campus environments.

Siveillance Vantage is an innovative and advanced software solution for mission critical security command and control centers operating critical infrastructure applications.

Solid Edge is a portfolio of software tools that addresses various product development processes : 3D design, simulation, manufacturing and design management.

Spectrum Power provides basic components for SCADA, communications, and data modeling for control and monitoring systems. Application suites can be added to optimize network and generation management for all areas of energy management.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2021-44228

Apache Log4j V2, versions < 2.15.0 do not protect JNDI features (as used in configuration, log messages, and parameters) against attacker controlled LDAP and other JNDI related endpoints.

An attacker who can control log messages or log message parameters could execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

This advisory will be updated as more information becomes available.

The following Siemens products are under active investigation to determine whether they are affected by CVE-2021-44228:

- Capital (and its derivatives)
- Comos Desktop App
- EnergyIP
- Geolus
- HCRA
- HES UDIS
- RUGGEDCOM ELAN
- RUGGEDCOM MAESTRO
- SINAMICS TEC - SDK
- SINUMERIK Analyze MyWorkpiece / Capture
- SINUMERIK Optimize MyMachine
- SiPass Integrated
- SIZER Design Tool for SINAMICS
- Spectrum Power
- Solid Edge
- Solid Edge Technical Publications
- Solid Edge Wiring and Harness Design
- Teamcenter
- XHQ

For more details regarding the Log4j vulnerability CVE-2021-44228 refer to https://logging.apache.org/log4j/2.x/security.html

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2021-12-13): Publication Date

TERMS OF USE