SSA-714170: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to SPPA-T3000

Publication Date:	2021-12-16
Last Update:	2022-02-08
Current Version:	V1.1
CVSS v3.1 Base Score:	10.0

SUMMARY

On 2021-12-09, a vulnerability in Apache Log4j (a logging library 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”.

On 2021-12-14 an additional denial of service vulnerability (CVE-2021-45046) was published rendering the initial mitigations and fix in version 2.15.0 as incomplete under certain non-default configurations. Log4j versions 2.16.0 and 2.12.2 are supposed to fix both vulnerabilities.

On 2021-12-17, CVE-2021-45046 was reclassified with an increased CVSS base score (from 3.7 to 9.0). The potential impact of CVE-2021-45046 now includes - besides denial of service - also information disclosure and local (and potential remote) code execution.

Siemens Energy is preparing updates and recommends specific countermeasures for SPPA-T3000.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SPPA-T3000 SeS3000 Security Server (6DU7054-0..00-..A0): All versions	Currently no remediation is available Specific mitigations and how to apply are described in the SE Controls Security Announcement Incident 2021-01, available in the customer portal. https://cep.siemens-energy.com/cep/ 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:

- Ensure that SPPA-T3000 is set up according to the security concept defined in the SPPA-T3000 security manual

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid’s reliability can thus be minimized by virtue of the grid design.

Siemens Energy strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens

Energy strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens Energy strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

SPPA-T3000 SeS3000 Security Server provides the possibility to centrally deploy updates and security patches for SPPA-T3000.

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

Vulnerability CVE-2021-45046

The fix to address CVE-2021-44228 was incomplete in certain non-default configurations, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, ${ctx:loginId}).

This could allow attackers with control over Thread Context Map (MDC) input data to craft malicious input data using a JNDI Lookup pattern, resulting in an information leak and remote code execution in some environments and local code execution in all environments.

CVSS v3.1 Base Score	9.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

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 (2021-12-16):	Publication Date
V1.1 (2022-02-08):	Revised severity of CVE-2021-45046; added specific document title provided in Siemens Energy customer portal

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.