Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

SICK Security Advisory for Apache Log4j (CVE-2021-44228)

Document ID:	SCA-2021-0003
Publication Date:	2021-12-17
CVE Identifier:	CVE-2021-44228
CVSSv3 Base Score:	10
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Version:	7

List of Products

Product	Part Number	Affected by
SICK AppManager <1.5.0		CVE-2021-44228 Status: Fixed Remediation: Vendor fix
SICK AppStudio <3.6.0	1610199	CVE-2021-44228 Status: Fixed Remediation: Vendor fix
SICK FieldEcho <1.5.3	1612993	CVE-2021-44228 Status: Fixed Remediation: Vendor fix
SICK FieldEcho Dashboard <1.2.2		CVE-2021-44228 Status: Fixed Remediation: Vendor fix
SICK Function Block Factory <1.4.1		CVE-2021-44228 Status: Fixed Remediation: Vendor fix

Vulnerability Overview

CVE-2021-44228 Deserialization of Untrusted Data

Summary: A critical remote code execution vulnerability impacting at least Apache Log4j 2 (versions 2.0 to 2.14.1) was recently announced by Apache. This vulnerability is designated by Mitre as CVE-2021-44228 with the highest severity rating of 10.0. The vulnerability is also known as Log4Shell by security researchers. If exploited, this vulnerability allows adversaries to potentially take full control of the impacted system. Log4j 2 is a commonly used open source third party Java logging library used in software applications and services.

CVE-2021-44228 has been assigned to this vulnerability.
CVSSv3.1 base score: 10
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-502 (Deserialization of Untrusted Data)

References:
Apache Security Advisory:
https://logging.apache.org/log4j/2.x/security.html

CVE Entry:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Remediations

Vendor Fix for CVE-2021-44228

Details: Fixed on vendorside

Valid for:

- SICK AppManager <1.5.0
- SICK AppStudio <3.6.0
- SICK FieldEcho <1.5.3
- SICK FieldEcho Dashboard <1.2.2
- SICK Function Block Factory <1.4.1

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://sick.com/psirt

SICK Operating Guidelines:
https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.PDF

ICS-CERT recommended practices on Industrial Security:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

Additional Product Information

SICK AppManager <1.5.0	Product on sick.com: https://www.sick.com/de/de/p/p532784
SICK AppStudio <3.6.0	Product on sick.com: https://www.sick.com/de/de/p/p448644
SICK FieldEcho <1.5.3	Product on sick.com: https://www.sick.com/de/de/p/p597264
SICK FieldEcho Dashboard <1.2.2	Product on sick.com: https://www.sick.com/de/de/p/p651603
SICK Function Block Factory <1.4.1	Product on sick.com: https://www.sick.com/de/de/p/p653518

History

Version	Release Date	Comment
1	2021-12-14	Initial Release
2	2021-12-16	Updated affected products
3	2021-12-17	Updated affected versions
4	2022-01-14	Updated affected products
5	2022-01-19	Updated affected products
6	2022-02-17	Updated affected products
7	2023-02-10	Updated Advisory (only visual changes)