



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: 8

### List of Products

---

Product	Part Number	Affected by
<b>SICK AppManager &lt;1.5.0</b>		<a href="#">CVE-2021-44228</a> Status: Fixed Remediation: Vendor fix
<b>SICK AppStudio &lt;3.6.0</b>	1610199	<a href="#">CVE-2021-44228</a> Status: Fixed Remediation: Vendor fix
<b>SICK FieldEcho &lt;1.5.3</b>	1612993	<a href="#">CVE-2021-44228</a> Status: Fixed Remediation: Vendor fix
<b>SICK FieldEcho Dashboard &lt;1.2.2</b>		<a href="#">CVE-2021-44228</a> Status: Fixed Remediation: Vendor fix
<b>SICK Function Block Factory &lt;1.4.1</b>		<a href="#">CVE-2021-44228</a> Status: Fixed Remediation: Vendor fix

**TLP:WHITE**

## 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://www.sick.com/media/docs/9/19/719/special\\_information\\_sick\\_operating\\_guidelines\\_cybersecurity\\_by\\_sick\\_en\\_im0106719.pdf](https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.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

---

<b>SICK AppManager &lt;1.5.0</b>	Product on sick.com: <a href="https://www.sick.com/de/de/p/p532784">https://www.sick.com/de/de/p/p532784</a>
<b>SICK AppStudio &lt;3.6.0</b>	Product on sick.com: <a href="https://www.sick.com/de/de/p/p448644">https://www.sick.com/de/de/p/p448644</a>
<b>SICK FieldEcho &lt;1.5.3</b>	Product on sick.com: <a href="https://www.sick.com/de/de/p/p597264">https://www.sick.com/de/de/p/p597264</a>
<b>SICK FieldEcho Dashboard &lt;1.2.2</b>	Product on sick.com: <a href="https://www.sick.com/de/de/p/p651603">https://www.sick.com/de/de/p/p651603</a>

**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)
8	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated