PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

06 January 2022
300536911

Statement on Security Vulnerability “Log4Shell” discovered in Java library Log4J

Summary

Phoenix Contact has become aware of a new vulnerability in Apache Log4j also known as "Log4Shell" which is being actively exploited.

We have examined our product portfolio with the following result:

Physical products containing firmware	Not affected
Software products	Not affected
Cloud Services	Affected Services have been patched, no exploits have been observed.

General recommendation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Measures to protect network-capable devices with Ethernet connection

Vulnerability Classification

CVE-2021-44228:

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
CWE CWE-20: Improper Input Validation

CVE-2021-45046

CVSS v3.1 Base Score 3.7
CVSS Vector CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE CWE-20: Improper Input Validation

CVE-2021-44832:

CVSS v3.1 Base Score 6.6
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
CWE CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE CWE-20: Improper Input Validation

Additional Information

https://logging.apache.org/log4j/2.x/security.html

https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce

BSI - Kritische Schwachstelle in Java-Bibliothek log4j (bund.de)

Document revisions

Revision	Date	Remark
1.0	15.12.2021	Initial Release
1.1	06.01.2022	CVE added, Updated Summary section