MR Product CERT: ProductCERT@reinhausen.com

Security Advisory MRSA-2021-1201: Software vulnerability log4j

Version 5.0 - 28.01.2022

Summary

The critical vulnerability (Log4Shell) in the widely used Java library log4j leads to an extremely critical threat situation, according to the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) [1].

The vulnerability documented in CVE-2021-44228 is classified with a CVSS score of 10.0 [2].
The vulnerability documented in CVE-2021-45056 is classified with a CVSS score of 9.0 [3][4].
The vulnerability documented in CVE-2021-45105 is classified with a CVSS score of 7.5 [5].
The vulnerability documented in CVE 2021-44832 is classified with a CVSS score or 6.6 [6].
The vulnerability documented in CVE-2022-23302 is classified with a CVSS score or 8.8 [7].
The vulnerability documented in CVE-2022-23305 is classified with a CVSS score or 9.8 [8].
The vulnerability documented in CVE-2022-23307 is classified with a CVSS score or 9.8 [9].

Maschinenfabrik Reinhausen provides its customers with products of high quality and without vulnerabilities.

In light of the currently disclosed vulnerability in the software component "log4j", impact of this vulnerability has been assessed and actions to address it have been initiated where necessary. This publication informs you about the status and necessary steps if required.

Products

- Reviewed, not affected:
  - ETOS / ISM – all versions
  - HighVolt Customer Portal – https://portal.highvolt.com/
  - MR Customer Portal - https://portal.reinhausen.com/
  - MESSKO® Download Center - https://messko-download.reinhausen.com/
  - MControl 7“ and 10“
  - TESSA Fleetscan
  - TESSA APM
  - TAPCON 230, 240, 250, 260, ISM – all versions
  - TAPGUARD 240, 260
  - TRAFOGUARD T24
  - MR Suite (TAPCON-trol, TRAFOVISOR® and TRAFOSET™)
  - MTeC® EPT202, EPT303, EPT303 FO
  - MTraB® - all versions
  - MSET Configuration for MSENSE® DGA, MTRAB®, MSENSE® FO
  - MLOG and MLOG-Analyzer
  - MSENSE® DGA (2 / 3 / 5 / 9)
  - MSENSE® FO
  - ECOTAP® VPD® - all versions
  - TT30

    - SW 3-3

- Reviewed, affected:
    - None

- In review:
    - None

Description

To successfully exploit these software vulnerabilities an attacker must inject specifically formatted code into the software system, which then leads to unauthorized network connections, download of possibly malicious codes and subsequent execution. The impact results in a loss of availability of the system as well as confidentiality and integrity of stored information on the vulnerable system. This can be used to steal login credentials, raise local privileges or perform lateral movement and compromise of further systems.

General recommendations on IT Security

- Ensure that only authorized personnel have access to the device.
- Only use the device within an ESP (electronic security perimeter). Do not connect the device to the Internet in an unprotected state. Use mechanisms for vertical and horizontal network segmentation and security gateways (firewalls) at the transition points.
- Ensure that the device is only operated by trained personnel who are familiar with IT security.
- Check regularly whether software updates are available for the device and perform the updates.

Change history

- 1.0: Initial release as of December 16th 2021
- 2.0: Include statement and review for second log4j vulnerability CVE-2021-45056 and CVE-2021-45105. Add/update statement for Highvolt Customer Portal, MTeC® EPT303 and MTeC® EPT303 FO, MSET Configuration for MSENSE® DGA, MTRAB®, MSENSE® FO, MLOG, MLOG-Analyzer, MSENSE® FO, SW 3-3, MR Suite, TAPCON-trol, TRAFOVISOR® and TRAFOSET™.
  Add URL for Messko Customer / Download Portal. MR Customer Portal and Messko Download Portal need more review for second and third vulnerability. CVSS Score of CVE-2021-45056 was adjusted from 3.7 to 9.0. Released December 20th 2021.
- 3.0: MR Customer Portal is not vulnerable to the recent CVEs. Released December 22nd 2021.
- 4.0: Review and update statement for vulnerability CVE 2021-44832, Messko Customer / Download Portal was checked with no log4j vulnerability found. Released January 17th 2022.
- 5.0: Three new CVEs that were published have been evaluated, no products and services are affected. Released 28.01.2022.

Additional information

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Warnstufe Rot: Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage.
URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html

[2] National Vulnerability Database: CVE-2021-44228.
URL: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[3] National Vulnerability Database: CVE-2021-45056.
URL: https://nvd.nist.gov/vuln/detail/CVE-2021-45046/

[4] The Apache Software Foundation: Apache Log4j Security Vulnerabilities.
URL: https://logging.apache.org/log4j/2.x/security

[5] National Vulnerability Database: CVE-2021-45105.
URL: https://nvd.nist.gov/vuln/detail/CVE-2021-45105

[6] National Vulnerability Database: CVE-2021-44832.
URL: https://nvd.nist.gov/vuln/detail/CVE-2021-44832

[7] National Vulnerability Database: CVE-2022-23302.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-23302

[8] National Vulnerability Database: CVE-2022-23305.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-23305

[9] National Vulnerability Database: CVE-2022-23307.
URL: https://nvd.nist.gov/vuln/detail/CVE-2022-23307