Security Advisory MRSA-2024-0401: Software vulnerability xz

Version 1.1 - 09.04.2024

Summary

A backdoorin a compromised version of the xz package and the associated liblzma library can be used to execute arbitrary commands via ssh under some special conditions[1][2].

The vulnerability documented in CVE-2024-3094 is classified with a CVSS score of 10.0[3]

Maschinenfabrik Reinhausen provides its customers with products of high quality and without vulnerabilities. Considering the currently disclosed vulnerability in the software components xz and its result on ssh, 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
  - TAPCON 230, 240, 250, 260, ISM – all versions
  - MControl 7“ and 10“
  - myReinhausen customer portal - https://portal.reinhausen.com/
  - TESSA APM Oil
  - 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

A backdoor was placed in the xz software in the process of creating binary-only release tarballs by one of its maintainers, with the malware being only present in those release tarballs, not in the source code (github repository) itself. When used, the malicious tarball would – in interaction with Secure Shell (ssh) logins – allow a remote attacker holding special login credentials unauthorized access to the system with system level privileges. This would allow to execute arbitrary commands and compromise the systems with the following possible impact:

- Unauthorized access to the system with system-level privileges (root)
- Full compromise of system confidentiality, integrity, and availability
- Potential lateral movement to attack other systems (nearby or remote)

The requirements for a successful attack include using the malicious tarball or xz versions 5.6.0 and 5.6.1 which was only online a few days before detection. In that timeframe, the malicious tarball was included in very few software products, i.e. various Linux distributions. None of those vulnerable software products are used in any of our products.

As such no vulnerabilities are present in any of the MR products.

Software Updates

No software update is required.

General recommendations on IT Security

- Ensure that only authorized personnel have access to the device.
- Only use the device within an electronic security perimeter (ESP). 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

- 0.1: First draft of a security advisory as of April 3rd 2024.
- 1.0: Added more reviewed products, publish on April 4th 2024.
- 1.1: Several changes regarding status of products by Maschinenfabrik Reinhausen:
  - The following products were tested and no vulnerabilities found: 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;.
  - Revised description.
  - Published on April 9th 2024

Additional information

[1] Bundesamt für Sicherheit in der Informationstechnik: Kritische Backdoor in XZ für Linux.
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-223608-1032.html

[2] Open Source Security Foundation: xz Backdoor CVE-2024-3094.
https://openssf.org/blog/2024/03/30/xz-backdoor-cve-2024-3094/

[3] National Vulnerability Database: CVE-2024-3094.
https://nvd.nist.gov/vuln/detail/CVE-2024-3094