TRUMPF Werkzeugmaschinen SE + Co. KG
Johann-Maus-Straße 2 · 71254 Ditzingen · Germany

VDE-CERT

TRUMPF Werkzeugmaschinen SE + Co. KG

Johann-Maus-Straße 2
71254 Ditzingen

Phone +49 7156 303-0
Fax +49 7156 303-30309

info@trumpf.com
www.trumpf.com

Your contact
Phone extension
Fax extension
E-Mail: product.security@trumpf.com
Date: 23.01.2024

Multiple TRUMPF products include a vulnerable version of Notepad++ (VDE-2024-003)

CVE Identifiers

CVE-2023-40031
CVE-2023-40036
CVE-2023-40164
CVE-2023-40166

Severity

CVE-2023-40031: 7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

Affected Vendors

TRUMPF Werkzeugmaschinen

Affected Products

- TruTops Fab (Storage) up to and including V22.7
- Oseon up to and including V3.0.24

Vulnerability Type

BUFFER COPY WITHOUT CHECKING SIZE OF INPUT (CWE-120)
HEAP-BASED BUFFER OVERFLOW (CWE-122)

Summary

The TRUMPF products that are listed above contain a vulnerable version of Notepad++. This version is being installed for support purposes only, so there is no danger of triggering this vulnerability in Notepad++ during normal operations. Nevertheless, TRUMPF recommends mitigation of this vulnerability.
When editing a specially crafted file containing UTF-8 characters in Notepad++ (Versions up to 8.5.6)

and converting that file to UTF-16, a buffer overflow vulnerability can be exploited that allows an attacker to execute arbitrary code to take over the whole system.

Impact

A user who's editing and converting a specially crafted file using the vulnerable Notepad++ version in the TRUMPF product listed above can allow an attacker to execute code on the local server. This can impact confidentiality, integrity and availability of information on the affected system.

Solution

- Please download the replacement tool (LINK).
- For additional questions please contact your TRUMPF Service with the PR number 501709.

Reported by

TRUMPF coordinated with CERT@VDE