

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

VDE-CERT

TRUMPF 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
Date

30309
product.security@trumpf.com
14.11.2023

Multiple TRUMPF products prone to WIBU CodeMeter vulnerabilities

CVE Identifier

CVE-2023-3935

Severity

[9.8 \(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H\)](#)

Affected Vendors

TRUMPF Werkzeugmaschinen
TRUMPF Laser- und Systemtechnik

Affected Products

- TecZoneBend: from V18.02.R8 to V23.06.01
- TruTopsBoost: from V06.00.23.00 to V16.0.22
- TruTopsFab (inkl. TruTops Monitor): from V15.00.23.00 to V22.8.25
- Oseon: from V1.0.0 to V3.0.22
- TruTopsPrint: from V00.06.00 to V01.00
- TruTopsPrintMultilaserAssistant from V01.02
- ToPsCalculation: from V14.00 to V22.00.00
- TruTops: from V08.00 to V12.01.00.00
- TubeDesign: from V08.00 to V14.06.150
- ProgrammingTube V1.0.1 to V4.6.3
- TruTopsWeld from V7.0.198.241 to V9.0.28148.1

Managing Board:
Dr. phil. Nicola Leibinger-Kammüller (Chairwoman)
Dr. rer. pol. Lars Grünert
Dr.-Ing. Mathias Kammüller
Dipl.-Betriebsw. Oliver Maassen
Dr.-Ing. Stephan Mayer
Dr. rer. nat. Berthold Schmidt
Dr. rer. nat. Hagen Zimer

TRUMPF SE + Co. KG, Ditzingen, Commercial Register HRA 201460
(District Court Stuttgart), VAT ID. No. DE 146 019 590
Unlimited Liability Partner: Leibinger SE, Ditzingen,
Commercial Register HRB 777882 (District Court Stuttgart)
Chairman of the Supervisory Board: Dr.-Ing. E. h. Peter Leibinger

- TruTops Cell SW48 from V01.00 to V02.26.0
- TruTops Cell Classic to V09.09.02
- TruTops Mark 3D from V01.00 to V06.01
- MonitoringAnalyzer from V1.0 to V1.3
- Tops Unfold V05.03.00.00
- TruTopsFab_Storage_SmallStore from V14.06.20 to V20.04.20.00
- TrumpfLicenseExpert from V1.5.2 to V1.11.1

Vulnerability Type

OUT-OF-BOUNDS-WRITE (CWE-787)

Summary

The TRUMPF CAD/CAM software tools mentioned above use the vulnerable CodeMeter Runtime (up to version 7.60b) application from WIBU-SYSTEMS AG to manage licenses within the component TRUMPF License Expert. This CodeMeter application contains new vulnerabilities, which may enable an attacker to gain full access to the server or workstation on which the TRUMPF License Expert has been installed on. A new version of the TRUMPF License Expert which fixes these vulnerabilities is available.

Machines with a running and correctly installed mGuard hardware firewall cannot be exploited by this vulnerability if used as intended (according to the manual).

Impact

An attacker exploiting the vulnerabilities in WIBU CodeMeter Runtime in server mode could gain full access to the affected server via network access without any user interaction.

Exploiting the vulnerabilities in WIBU CodeMeter Runtime in non-networked workstation mode could lead to a privilege elevation and full access on this workstation for an already authenticated user (logged in locally to the PC).

In detail, the vulnerabilities are as follows:

Update A, 2023-11-13

Removed CVE-2023-4701 because it was revoked.

CVE-2023-3935

CWE-787 Out-of-bounds Write

CVSSv3.1 base score 9.8

CVSSv3.1 Vector 9.8 [\(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H\)](#)

Solution

Mitigation:

- Implement general security best practices like network segmentation, endpoint protection and system hardening.
- Restrict network access to the TRUMPF License Expert server component to required clients only by using firewalls or other suitable products.

Remediation:

- Get the latest version of the TRUMPF License Expert software ($\geq$ V2.0.0) [here](#) and install it on all affected servers and workstations.

Reported by

WIBU-SYSTEMS AG