TRUMPF Laser GmbH • Postfach 5 72 • 78707 Schramberg • Deutschland

VDE-CERT

**TRUMPF Laser GmbH**

Aichhalder Straße 39
78713 Schramberg

Telefon +49 7422 515-0
Telefax +49 7422 515-108

info@de.trumpf.com
www.trumpf.com

Ihr Ansprechpartner
Telefon direkt
Telefax direkt
E-Mail product.security@trumpf.com
Datum 07.11.2022

# Multiple TRUMPF products prone to X.Org server vulnerabilities

**VDE 2022-049**

TRUMPF-Security-Advisory-TSA-2022-4

## *CVE Identifier*

CVE-2022-2319, CVE-2022-2320

## *Severity*

7.8 (CVSS:3.1:AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

## *Affected Vendors*

TRUMPF Laser GmbH

## *Affected Products*

- TruPulse
- TruDisk
- TruDiode
- TruFiber
- TruMicro2000
- TruMicro5000
- TruMicro6000
- TruMicro7000
- TruMicro8000
- TruMicro9000
- redpowerDirect

TRUMPF Laser GmbH
Postfach 5 72 · 78707 Schramberg · Deutschland

with TruControl version as from 1.60.0 to 3.40.0

## *Vulnerability Type*

Out-of-bounds Write (CWE-787)

Improper Protection for Out of Bounds Signal Level Alerts (CWE-1320)

## *Summary*

TruControl laser control software from versions 1.60.0 to 3.40.0 use X.Org server versions affected by CVE-2022-2320 and CVE-2022-2319. The affected X.Org vulnerability is not validating the request length properly for the handler “ProcXkbSetGeometry” which could lead to memory out-of bounds write

## *Impact*

To be able to exploit this vulnerability the attacker first needs to gain any kind of user access to the system.

When logged on to the system the privilege escalation vulnerability can be exploited with following possible impacts/damages to the system:

- Data loss in the laser control
- Standstill of production
- Damage by change of the laser control

Safety is not affected since it is controlled by an independent electromechanical safety mechanism.

Remote Code Execution as one of the mentioned impacts in the vulnerability description of CVE-2022-2320 is not possible since no SSH Forwarding is used.

## *Solution*

**Mitigation:**

- Securing the access to the production network
- Please contact your service partner (service.tls@trumpf.com) for instructions on how to get automatically informed for the new major release 3.42.0 of the new TruControl software version

**Remediation:**

- Retrieve instructions on how to deactivate the ssh access or activate the firewall on port 22 (SSH) of your laser

## *Reported by*

CERT@VDE coordinated with TRUMPF Laser GmbH
Jan-Niklas Sohn working with Trend Micro Zero Day Initiative