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 22.03.2021

Multiple TRUMPF products prone to sudo vulnerability

CVE Identifier

CVE-2021-3156

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

with TruControl version as from 2.14.0 to 3.14.0

TRUMPF Laser GmbH
Postfach 5 72 · 78707 Schramberg · Deutschland

Vulnerability Type

Out-of-bounds Write (CWE-787)

Summary

TruControl laser control software from versions 2.14.0 to 3.14.0 use sudo versions affected by CVE-2021-3156. The affected sudo has a heap-based buffer overflow, allowing privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

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.

Solution

- Update to TruControl version 3.16.0 or higher or
- Please contact your service partner (service.tls@trumpf.com) for instructions on how to retrieve the patch

Reported by

Qualys Research Labs