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

VDE-CERT

TRUMPF GmbH + 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: 2021-12-15, 10:00 CET
Last updated on: 2021-12-17, 14:00 CET

TRUMPF Security Information for Apache Log4J, CVE-2021-44228

CVE Identifier

CVE-2021-44228

Severity

10.0 (CVSS:3.0:AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Affected Vendors

TRUMPF Werkzeugmaschinen

TRUMPF Laser- und Systemtechnik

Affected Products

TRUMPF is continuing to investigate any potential impact on TRUMPF-managed services, including myTRUMPF. If, as the investigation continues, any TRUMPF-managed services are found to be affected by this issue, TRUMPF will take immediate action to remediate the problem. Customers using TRUMPF-managed cloud services do not need to take any action.

In parallel, TRUMPF is investigating the potential impact on customer-managed (on-premises) products. Please find below the present status of these products:

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

Not affected products (in currently supported versions)

Machines & Systems	TruBend series
	TruLaser series
	TruPunch series
	TruMatic series
	other TRUMPF machines and systems
Laser	TruPulse
	TruDisk
	TruDiode
	TruFiber
	TruMark
	TruMicro series
	redpowerDirect
Sensor Systems	TRUMPF Visionline
	TRUMPF Seamline Remote
Software	TruTops Boost *(added 2021-12-16)*
	TruTops Calculate
	TruTops Classic
	TruTops Cell
	TruTops FAB *(added 2021-12-16)*
	TruTops Mark 3D
	TruTops Monitor
	TruTops Print Multilaser Assistant
	TruTops Print
	TruPrint Monitoring Analyzer
	TruTops PFO
	TruTops I-PFO
	PFO Smart Teach App
	QDS 2.0
	Smart View Services
	Smart Power Tube
Generators / Plasma Excitation	TruHeat *(added 2021-12-17)*
	TruPlasma *(added 2021-12-17)*
	TruConvert *(added 2021-12-17)*

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

Products still under investigation

TRUMPF finished the investigation on 17.12.2021 with no currently supported products being vulnerable.

Vulnerability Type

Improper Input Validation (CWE 20)
Uncontrolled Resource Consumption (CWE 400)
Deserialization of Untrusted Data (CWE 502)

Summary

Several TRUMPF products make use of 3rd party and open-source software components.
One open-source component, Log4J, can easily be tricked into connecting to an attacker-controlled server on the internet to download malicious code and execute it on the system it is running on. In addition, other, less severe attack scenarios are possible.
TRUMPF is currently investigating which machines, lasers and other products are affected by this vulnerability. This document will be continuously updated.

Impact

Currently, no impacts on TRUMPF machines, lasers, or on-prem products are known.

Solution

- Use the updated versions of affected TRUMPF on-prem products that will be available via your service channel shortly.
- Until then, reduce internet usage on workstations with potentially affected TRUMPF on-prem products to a minimum.

Reported by

Chen Zhaojun of Alibaba Cloud Security
Coordinated by CERT@VDE, CISA and BSI