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 13.08.2021

TRUMPF Laser GmbH: multiple products prone to codesys runtime vulnerabilities

CVE Identifier

CVE-2021-29242, CVE-2021-29241, CVE-2019-5105, CVE-2020-7052, CVE-2019-9012, CVE-2019-9010, CVE-2019-9009, CVE-2018-10612

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 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 1.04 to 3.0.0 and TRUMPF Peripheral Bus. (TRUMPF Peripheral Bus is a system expansion of the fieldbus interfaces of a laser control.)

Vulnerability Type

Unverified Ownership (CWE-283)l

Summary

TruControl laser control software from versions 1.04 to 3.0.0 use codesys runtime versions affected by CVE-2021-29242, CVE-2021-29241, CVE-2019-5105, CVE-2020-7052, CVE-2019-9012, CVE-2019-9010, CVE-2019-9009, CVE-2018-10612

Impact

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

When the system is reachable over the network these vulnerabilities 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
- Interception of sensitive data

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

In detail, the vulnerabilities are as follows:

> **Advisory 2021-01** CODESYS Control Runtime system before 3.5.17.0 has improper input validation
> **CVE-2021-29242**
> **CWE-20** Improper Input Validation
> **CVSSv3.1 base score** 7.3
> **CVSSv3.1 Vector** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)
>
> Link to advisory
>
> **Advisory 2021-04** CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS)
> **CVE-2021-29241**
> **CWE-476** NULL Pointer Dereference
> **CVSSv3.1 base score** 7.5
> **CVSSv3.1 Vector** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
>
> Link to advisory

TRUMPF Laser GmbH
Postfach 5 72 · 78707 Schramberg · Deutschland

Advisory 2020-02 An exploitable memory corruption vulnerability exists in the Name Service Client functionality of 3S-Smart Software Solutions CODESYS GatewayService
CVE-2019-5105
CWE-787 Out-of-bounds Write
CVSSv3.1 base score 7.5
CVSSv3.1 Vector (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Link to advisory

Advisory 2020-01 CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition.
CVE-2020-7052
CWE-770 Allocation of Resources Without Limits or Throttling
CVSSv3.1 base score 6.5
CVSSv3.1 Vector (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

Link to advisory

Advisory 2019-06 A crafted request may cause an unhandled error in the affected CODESYS products which results in a denial-of-service condition.
CVE-2019-9009
CWE-20 Improper Input Validation
CVSSv3.1 base score 7.5
CVSSv3.1 Vector (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Link to advisory

Advisory 2019-03 A crafted communication request may cause uncontrolled memory allocations in the affected CODESYS products and may result in a denial-of-service condition
CVE-2019-9012
CWE-770 Allocation of Resources Without Limits or Throttling
CVSSv3.0 base score 7.5
CVSSv3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Link to advisory

Advisory 2019-02 The CODESYS Gateway does not correctly verify the ownership of a communication channel
CVE-2019-9010
NVD-CWE-noinfo
CVSSv3.0 base score 9.8
CVSSv3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Link to advisory

Advisory 2018-10 User access management and communication encryption is not enabled by default, which could allow an attacker access to the device and sensitive information, including user credentials
CVE-2018-10612
CWE-284, CWE-311, CWE-732 Incorrect Permission Assignment for Critical Resource, Missing Encryption of Sensitive Data, Improper Access Control
CVSSv3.0 base score 9.8
CVSSv3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

TRUMPF Laser GmbH
Postfach 5 72 · 78707 Schramberg · Deutschland

Link to advisory

Advisory 2018-07 A crafted communication request may cause an access violation in the affected CODESYS products and may result in a denial-of-service condition.

NVD-CWE-noinfo
CVSSv3.0 base score 6.5
CVSSv3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

Link to advisory

Advisory 2018-04 The CODESYS runtime system allows to access files outside the restricted working directory of the controller by online services

NVD-CWE-noinfo Directory traversal
CVSSv3.0 base score 9.9
CVSSv3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

Link to advisory

Advisory 2017-03 A crafted request may cause an access violation in the affected CODESYS products and may result in a denial-of-service condition
NVD-CWE-noinfo Access violation, remote DoS
CVSSv3.0 base score 7.5
CVSSv3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Link to advisory

Solution

- We highly recommend updating to TruControl version 3.16.0 or higher as soon as possible
- Please contact your service partner (service.tls@trumpf.com) for immediate instructions on how to retrieve the update

Reported by

CODESYS GmbH

TRUMPF Laser GmbH reported the vulnerability to CERT@VDE.