

■ CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: 3D-Vision-Sensors VSE*000-F400-B12-A1000 and VTE7500-F400-B12-A1500 – devices are affected by regreSSHion

VDE-ID VDE-2024-063
 Document ID TDOCT-9527_ENG
 Publication date 2024-10-08

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2024-6387	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

Severity

Identifier	Base Score and Vector
CVE-2024-6387	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected products

Item No.	Item	Version
70123992-100000	VSE1000-F400-B12-A1000	< 1.15.0.0
70123992-100001	VSE2000-F400-B12-A1000	< 1.15.0.0
70123992-100002	VSE3000-F400-B12-A1000	< 1.15.0.0
70123993-100000	VTE7500-F400-B12-A1500	< 1.15.0.0

Summary

The affected devices run a SSH server that is affected by the regreSSHion vulnerability despite the fact that no user can actually log in through SSH. Attackers may exploit this vulnerability to gain root access to the device.

Impact

An unauthenticated remote attacker can

- read files from the device
- modify or delete data on the device
- can interrupt the device functionality

Solution

Update to the Firmware version 1.15.0.0.

A firmware update will be made available shortly on the corresponding product page on the Pepper+Fuchs Homepage.

Reported by

Pepperl + Fuchs SE
Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.

