# CYBER SECURITY NOTIFICATION

## PEPPERL+FUCHS: Multiple VisuNet devices - Vulnerability may allow remote authorized attackers trigger a remote code execution

| | |
|---|---|
| Document ID | TDOCT-8158_ENG |
| Publication date | 2022-04-26 |

## Vulnerabilities

| Identifier | Vulnerability Type | Description |
|---|---|---|
| CVE-2022-21990 | NVD-CWE-noinfo, Insufficient Information | In the case of a Remote Desktop connection, an attacker with control of a Remote Desktop Server could trigger a remote code execution (RCE) on the RDP client machine when a victim connects to the attacking server with the vulnerable Remote Desktop Client. |

## Severity

| Identifier | Base Score and Vector |
|---|---|
| CVE-2022-21990 | 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) |

## Affected VisuNet products

| Item | RM Shell Version | OS Version |
|---|---|---|
| RM-GXP-*-T3-* | 5.x | Windows 10 LTSC 2019 |
| RM-320S-*-2-* | | |
| BTC12-*-TS3-* | | |
| BTC14-*-TS3-* | | |
| PAD-EX01P8DZ2EURC0508256WIFRMS | | |
| UPGRADE-TO-SHELL5-2019-LTSC* | | |
| RM-GXP-*-T2-* | 5.x | Windows 10 LTSC 2016 |
| BTC12-*-TS2-* | | |
| BTC14-*-TS2-* | | |
| RM2xx-*-T6-* | | |
| RM37xx-*-T6-* | | |
| RM9xx-*-T61-* | | |
| RM82xx-*-T61-* | | |
| RM87xx-*-T61-* | | |
| UPGRADE-RMSHELL4-TO-SHELL5* | | |
| RM32xx-*-T61-* | | |
| BTC11-*-TS2-* | | |
| BTC11-*-TS3-* | | |
| RM3207-*-T61-* | | |

A * summarizes the product variants.

## Summary

Critical vulnerabilities have been discovered in the utilized component Remote Desktop Client by Microsoft.

For more information see: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990

## Impact

Pepperl+Fuchs analyzed and identified affected devices.

In the case of a Remote Desktop connection, an attacker with control of a Remote Desktop Server could trigger a remote code execution (RCE) on the RDP client machine when a victim connects to the attacking server with the vulnerable Remote Desktop Client.

The impact of the vulnerabilities on the affected device may result in

- code execution

With the products mentioned above, the connection can only be established to RDP servers that have already been preconfigured by the role administrator or engineer. The role operator can therefore not connect to a random RDP server.

## Solution

The following external protective measured are required:

- Connect only to trusted RDP servers.
- Protect your RDP servers with anti-virus software and Intrusion Detection System (=IDS)
- Access control to RDP servers and the role administrator and engineer on the affected device.

## Reported by

Pepperl+Fuchs
Coordinated by CERT@VDE

## Support

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