Remote I/O fieldbus couplers (IP20) affected by INFRA:HALT vulnerabilities

Advisory

Document Identifyer:	D1505190
Version:	1.0
Publication Date:	2021-10-18
Reference:	VDE-2021-042

CVE Identifier

- CVE-2020-35683
- CVE-2020-35684
- CVE-2021-31401

Severity

- 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Affected Products

The following Weidmüller Remote I/O fieldbus couplers with the indicated firmware are affected:

Product number	Product name	Firmware version
1334890000	UR20-FBC-CAN	≤ 01.08.00
1334900000	UR20-FBC-DN	≤ 01.08.00
1334910000	UR20-FBC-EC	≤ 01.12.00
1334920000	UR20-FBC-EIP	≤ 02.11.00
1334940000	UR20-FBC-PL	≤ 01.08.00
2661310000	UR20-FBC-IEC61162-450	≤ 01.01.00
2476450000	UR20-FBC-MOD-TCP-V2	≤ 02.08.01
2566380000	UR20-FBC-PN-IRT-V2	≤ 01.11.00
2614380000	UR20-FBC-PB-DP-V2	≤ 01.10.00
2625010000	UR20-FBC-CC	≤ 01.00.02
2659680000	UR20-FBC-PN-ECO	≤ 01.00.02
2659690000	UR20-FBC-EC-ECO	≤ 01.00.01
2659700000	UR20-FBC-MOD-TCP-ECO	≤ 01.00.00
2680260000	UR20-FBC-CC-TSN	≤ 01.02.01

Vulnerability Type

Improper Input Validation (CWE-20)

Summary

The Weidmueller Remote I/O (IP20) fieldbus couplers (u-remote) are affected by several vulnerabilities of the third-party TCP/IP Niche stack. An attacker may use crafted IP packets to cause a denial of service or breach of integrity of the affected products. Weidmueller recommends restricting network access from the internet and also locally to reduce the attack vector to a manageable minimum.

Impact

CVE ID	CVE-2020-35683
Vulnerability Type	Improper Input Validation (CWE-20)
CVSS	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Description	An issue was discovered in HCC Nichestack 3.0. The code that parses ICMP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the ICMP checksum. When the IP payload size is set to be smaller than the size of the IP header, the ICMP checksum computation function may read out of bounds, causing a Denial-of-Service.

CVE ID	CVE-2020-35684
Vulnerability Type	Improper Input Validation (CWE-20)
CVSS	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Description	An issue was discovered in HCC Nichestack 3.0. The code that parses TCP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the length of the TCP payload within the TCP checksum computation function. When the IP payload size is set to be smaller than the size of the IP header, the TCP checksum computation function may read out of bounds (a low-impact write-out-of-bounds is also possible).

CVE ID	CVE-2021-31401
Vulnerability Type	Improper Input Validation (CWE-20)
CVSS	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Description	An issue was discovered in tcp_rcv() in nptcp.c in HCC embedded InterNiche 4.0.1. The TCP header processing code doesn't sanitize the value of the IP total length field (header length + data length). With a crafted IP packet, an integer overflow occurs whenever the value of the IP data length is calculated by subtracting the length of the header from the total length of the IP packet.

Solution

Fieldbuses (including Industrial Ethernet protocols) in general are not intended for direct connection to the internet, as they lack a proper set of security capabilities. This also applies to Weidmüller IP20 Remote I/O fieldbus couplers, which are developed and designed for operation in closed industrial networks.

Remediation

- Do not directly connect the affected products to the internet.
- Restrict network access to the affected products by proper secured network infrastructure (e.g. routers, firewalls, DMZ, VPNs).
- Restrict physical access to the industrial network and affected products (e.g cabinets, seals, closures).

Reported by

These vulnerabilities were discovered and reported by Forescout Technologies, Inc.

Weidmüller thanks CERT@VDE for the coordination and support with this publication.

Support
For support please contact Weidmüller at www.weidmueller.com/service.