Accidentally open network port in u-controls and IoT-Gateways

Advisory
Document Identifier: D1483156
Version: 1.0
Publication Date: 2021-05-04
Reference: VDE-2021-016

CVE Identifier
CVE-2021-20999

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

Affected Products
The following Weidmüller controls/gateways with the indicated firmware are affected:

Product number	Product name	Firmware version
1334950000	UC20-WL2000-AC	1.3.0 - 1.9.0, 1.10.0 - 1.10.2, 1.11.0, 1.12.1
1334990000	UC20-WL2000-IOT	
2682620000	IOT-GW30	
2682630000	IOT-GW30-4G-EU	

Vulnerability Type
Exposure of Resource to Wrong Sphere (CWE-668)

Summary
A network port intended only for device-internal usage is accidentally accessible via external network interfaces.

Impact
The reported vulnerability allows an attacker who has network access and knowledge about the internal configuration protocol to read and write configuration data without prior authorization. By exploiting this vulnerability the attacker potentially is able to manipulate or stop the operation of the device.

Solution

Mitigation

- Restrict access to the network the device is connected to.
- Do not directly connect the device to the internet.

Remediation

Weidmüller recommends upgrading affected devices to the current **firmware version 1.12.3 or higher** which fixes this vulnerability.

Alternatively the following firmware versions which fix this vulnerability may be installed:

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com

Product	Affected (installed) firmware version	Fixed firmware version
Any affected product	1.3.0 - 1.9.0	1.9.1
	1.10.1, 1.10.2	1.10.3
	1.10.0, 1.11.0, 1.12.1	1.12.3

Reported by
Reported by Weidmüller.

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

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com