Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

Phoenix Contact GmbH & Co. KG · 32825 Blomberg

100 years of passion for technology and innovation

11 April 2023
2023/00004

Security Advisory for ENERGY AXC PU, SMARTRTU AXC and Infobox

Publication Date: 2023-04-11
Last Update: 2023-04-11
Current Version: V1.0

Advisory Title

Directory Traversal Vulnerability enables arbitrary file access in ENERGY AXC PU Web service.

Advisory ID

VDE-2023-004
CVE-2023-1109

Vulnerability Description

An authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service.

Affected products

Article no	Article	Affected versions	Fixed version
1264327	ENERGY AXC PU	<= V04.15.00.00	V04.15.00.01

...

1110435	SMARTRTU AXC SG	<= V01.08.00.02	V01.09.00.00
1264328	SMARTRTU AXC IG	<= V01.02.00.01	End of Q3 2023
1169323	Infobox*	<= V02.02.00.00	not available

* Discontinued

Impact

The vulnerability enables an attacker to gain access to the file system of the devices. This can enable the attacker to compromise the device in terms of availability, integrity and confidentiality.

Classification of Vulnerability

CVE-2023-1109
Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-22

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

Temporary Fix / Mitigation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note.
Measures to protect network-capable devices with Ethernet connection

Remediation

Phoenix Contact strongly recommends updating to the latest firmware mentioned in the list of affected products, which fixes this vulnerability.

Acknowledgement

This vulnerability was discovered and reported by Laokoon SecurITy GmbH on behalf of E.ON Digital Technology GmbH.
We kindly appreciate the coordinated disclosure of this vulnerability by the finder.
PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2023-04-11): Initial publication