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

04 August 2021
300515639

Security Advisory for PLCnext Control devices

Advisory Title

Denial of service attack using special crafted JSON request

Advisory ID

CVE-2021-34570
VDE-2021-029

Vulnerability Description

A device on the same network as the controller sending a special crafted JSON request to the /auth/access-token endpoint may cause the controller to restart (CWE-20).

Affected products

Article no	Article	Affected versions	Fixed Version
1151412	AXC F 1152	< 2021.0.5 LTS	Download
2404267	AXC F 2152	< 2021.0.5 LTS	Download
1069208	AXC F 3152	< 2021.0.5 LTS	Download
1051328	RFC 4072S	< 2021.0.5 LTS	Download
1046568	AXC F 2152 Starterkit	< 2021.0.5 LTS	Download
1188165	PLCnext Technology Starterkit	< 2021.0 5 LTS	Download

Impact

An attacker could potentially script this request and create a denial of service attack condition.

Classification of Vulnerabilities

CVE-2021-34570

Update A: Corrected CVSS score and vector
Base Score: High 9.1
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

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 recommends affected users to upgrade to the current Firmware 2021.0.5 LTS or higher which fixes this vulnerability.

Acknowledgement

The vulnerability was discovered by Oliver Carrigan of Dionach.
We kindly appreciate the coordinated disclosure of these vulnerabilities by the finder.

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