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

17 December 2020
300494776/pbsa56

Security Advisory for PLCnext Control devices

Advisory Title

Multiple Vulnerabilities in PLCnext devices running firmware 2020.1 LTS: Authenticated stored Cross-Site-Scripting, unintended information disclosure, privilege escalation.

Advisory ID

CVE-2020-12517
CVE-2020-12518
CVE-2020-12519
CVE-2020-12521
VDE-2020-049

Vulnerability Description

CVE-2020-12517
Authenticated stored Cross-Site-Scripting vulnerabilities have been discovered at dedicated HTTP-parameters of the web interfaces: Improper Neutralization of Input (XSS) (CWE-79)

CVE-2020-12518
An authenticated low privileged user can read sensitive information: Exposure of Sensitive Information (CWE-200)

CVE-2020-12519
A system account without login rights can be utilized to execute shell commands with root privileges enabling the attacker to gain root access: Improper Privilege Management (CWE-269)

CVE-2020-12521
A specially crafted LLDP packet may lead to a high system load in the PROFINET stack: Improper Input Validation (CWE-20)

Affected products

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

Impact

CVE-2020-12517
An authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation).

CVE-2020-12518
An attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks.

CVE-2020-12519
An attacker can use this vulnerability i.e. to open a reverse shell with root privileges.

CVE-2020-12521
An attacker can cause failure of system services or a complete reboot.

Classification of Vulnerabilities

CVE-2020-12517
Base Score: High 8.8
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2020-12518
Base Score: 5.5
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2020-12519
Base Score: 8.8
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE-2020-12521
Base Score: 6.5
Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/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 LTS or higher which fixes these vulnerabilities.

Acknowledgement

The vulnerabilities CVE-2020-12517 to 12519 were discovered by Patrick Muench, Torsten Loebner, Maurice Rothe, Pascal Keul and Daniel Hackel of SVA Systemvertrieb Alexander GmbH.

We kindly appreciate the coordinated disclosure of these vulnerabilities by the finder.