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

16 April 2019
300424428/pbsa56

Security Advisories for AXC F 2152

Contents

Document revision

Revision	Date	Remark
1.0	2019-04-16	Initial Release
1.1	2019-05-28	CVSS-Vectors for CVE-2019-10997 and CVE-2019-10998 adjusted in consultation with CERT@VDE
1.2	2019-08-28	Added remediation option for SD-Card issue (page 6)

Security Advisory for AXC F 2152 Linux Components

Advisory Title

AXC F 2152 Firmware 1.x contains multiple Linux Components vulnerabilities.

Advisory ID

VDE-2019-009

Vulnerability Description

A check of AXC F 2152 firmware 1.x reports the usage of several older versions of 3rd party open source software components.
In the following table you can find the list of known vulnerabilities for some 3rd party open source components inside the firmware 1.x affecting AXC F 2152:

Component	Vulnerabilities
busybox	CVE-2016-6301
tcpdump	CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543
openssh	CVE-2017-15906
nginx	CVE-2016-1247
python	CVE-2018-1000117
libexpat	CVE-2017-9233
openssl	CVE-2017-3735, CVE-2017-3731, CVE-2017-3738, CVE-2017-3737, CVE-2018-0737
zlib	CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843
curl	CVE-2018-1000122, CVE-2018-1000301, CVE-2017-8817, CVE-2018-1000120, CVE-2018-1000121, CVE-2016-9952, CVE-2016-9953, CVE-2017-1000101, CVE-2017-8816, CVE-2017-1000254, CVE-2017-1000100, CVE-2017-1000257, CVE-2018-1000005, CVE-2016-7141
gnutls	CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444
strongswan	CVE-2017-9023, CVE-2018-5388, CVE-2017-9022, CVE-2017-11185
jquery	CVE-2015-9251, CVE-2016-7103

...

Affected products

- AXC F 2152 - article number 2404267
- Starterkit - AXC F 2152 STARTERKIT - article number 1046568

Impact

Availability, integrity, or confidentiality of the AXC F 2152 might be compromised by attacks using these vulnerabilities.

Remediation

Update to Firmware Release 2019.0 LTS or later.
Update to PLCnext Engineer Release 2019.0 LTS or later.

The Firmware Release 2019.0 LTS uses an updated Linux Version.

Acknowledgement

These vulnerabilities were discovered with the support of https://firmalyzer.com/.

Security Advisory for AXC F 2152 Denial-of-Service

Advisory Title

Denial-of-Service-Attack possible on AXC F 2152 FW 1.x using PC WORX Engineer communication port.

Advisory ID

CVE-2019-10997
VDE-2019-009

Vulnerability Description

Protocol Fuzzing on PC WORX Engineer by a man in the middle attacks stops the PLC service. The device must be rebooted, or the PLC service must be restarted manually via Linux shell.

Affected products

- AXC F 2152 - article number 2404267 using Firmware 1.x
- Starterkit - AXC F 2152 STARTERKIT - article number 1046568 using Firmware 1.x

Impact

PLC service is stopped the PLC program is not executed anymore.

Classification of Vulnerability

Base Score:7.5 HIGH
Vector: CVSS3.0:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Remediation

Update to Firmware Release 2019.0 LTS or later.
Update to PLCnext Engineer Release 2019.0 LTS or later.

Potential man in the middle attacks between the PLCnext Engineer and the AXC F 2152 are recognized by the PLCnext Engineer now. The user has the choice to stop the connection or to continue if the communication breach is intended and needed to support the chosen network architecture.

Acknowledgement

This vulnerability was discovered and reported by Zahra Khani (Firmalyzer SPRL).

Security Advisory for AXC F 2152 SD card usage

Advisory Title

Physical access to SD card enables authentication bypass opportunity.

Advisory ID

CVE-2019-10998
VDE-2019-009

Vulnerability Description

State of the art PLC devices offer SD cards to store the PLC's data.
In case of hardware failure easy and fast hardware replacement is required in industrial applications.
Replacement of the SD card without any additional tools and knowledge about the PLC or PLCs toolchain as well as automatic startup is a must.
To support this handling the physical access to the PLC device must be restricted by organizational measurements (e.g.: locked cabinets or other limited accesses)

In special use cases it might be not possible to effectively restrict access to authorized personal.
In such application scenarios, manipulation of the SD card is possible.

Affected products

- AXC F 2152 - article number 2404267 using Firmware 1.x
- Starterkit - AXC F 2152 STARTERKIT - article number 1046568 using Firmware 1.x

Impact

Unlimited access to the PLC may lead to a manipulation of SD cards data. This could allow an attacker to bypass the authentication of the device.

Classification of Vulnerability

Base Score:6.8 Medium
Vector: CVSS3.0:AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Temporary Fix / Mitigation

Please follow the advises according the SD card usage in the manual:
Art.-Nr. 107708: UM EN AXC F 2152 Installing, starting up, and operating the AXC F 2152 controller um_en_axc_f_2152_107708_en_02.pdf

In addition, it is recommended to use the Notification Manager to monitor SD card exchanges by the application program.

Remediation

Update to Firmware Release 2019.0 LTS or later
Update to PLCnext Engineer Release 2019.0 LTS or later

Update Rev 1.2: With Firmware Release 2019.6 an option was added to the web-based management that allows the user to permanently disable storage of configuration data to the SD-Card. The device can now be operated without SD-Card and ignores any inserted SD-Card. We recommend using this new configuration option for application scenarios where physical access to the device cannot be restricted effectively.

Acknowledgement

This vulnerability was discovered and reported by Zahra Khani (Firmalyzer SPRL).

Security Advisory for AXC F 2152 OPC UA Server Basic128Rsa15 security policy

Advisory Title

User Authentication Token Exploit OPC UA CVE-2018-7559.

Advisory ID

CVE-2018-7559
VDE-2019-009

Vulnerability Description

The OPC Foundation has published CVE-2018-7559 with a Security Bulletin on April 12, 2018. This vulnerability affects the handling of UserIdentityTokens when used with the Basic128Rsa15 security policy. The vulnerability allows an attacker to decrypt a previously captured password or to sign arbitrary data.
The Basic128Rsa15 security policy is deprecated by the UA Specification since July 2015, therefore it is recommended not to use this policy any longer.

Affected products

- AXC F 2152 - article number 2404267 using Firmware 1.x
- AXC F 2152 STARTERKIT - article number 1046568 using Firmware 1.x

Impact

This security vulnerability in OPC UA Server can allow a remote attacker to exploit a Server's private key by sending carefully constructed UserIdentityTokens encrypted with the Basic128Rsa15 security policy. It affects client and server applications and could allow an attacker to decrypt passwords even if they are encrypted with another security policy such as Basic256Sha256

Classification of Vulnerability

Base Score: 7.6 High
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L

Remediation

1. Disable Basic128Rsa15 Security Policy in OPC Servers configuration.
   Use only Basic256 or higher.

2. Update to Firmware Release 2019.0 LTS or later.
   Update to PLCnext Engineer Release 2019.0 LTS or later.

   The encryption method Basic128RSA15 is switched off by default in these releases.

Acknowledgement

We thank the OPC Foundation for publishing this CVE.

General Recommendation

Customers using Phoenix Contact AXC F 2152 are recommended to operate the 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:
Art.-Nr. 107913: AH EN INDUSTRIAL SECURITY “Measures to protect network-capable devices with Ethernet connection against unauthorized access”