TLP:WHITE

VDE-2024-022: Security Advisory for CHARX-SEC3xxx Charge controllers

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Aug 13 12:00:00 CEST 2024	Engine: 2.5.8
Current release date: Tue Aug 13 12:00:00 CEST 2024	Build Date: Wed Jul 24 07:54:41 CEST 2024
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 8.6	Severity: high
Original language:	Language: en-GB
Also referred to: VDE-2024-022, PCSA-2024/00003	

Summary

Start sequence for firewall service allows attack during the boot process. Password is reset to default when the device undergoes a firmware upgrade.

General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security

Impact

These vulnerabilities may allow an attacker within the network to change the device configuration through an unauthenticated internal service before the firewall is started during boot process. The second vulnerability may allow an local attacker to use the firmware update feature to reset the user-app accounts password to the dafault value that is documented in the product documentation. The user "user-app" has limited access rights.

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 General Recommendation.

Remediation

Phoenix Contact strongly recommends upgrading affected charge controllers to firmware version 1.6.3 or higher which fixes these vulnerabilities.

Product Description

CHARX control modular AC are charging controllers for mode 3 electric vehicle charging.

Summary

Start sequence for firewall service allows attack during the boot process. Password is reset to default when the device undergoes a firmware upgrade.

Product groups

Affected Products.

- Firmware < 1.6.3 installed on CHARX SEC-3000
- Firmware < 1.6.3 installed on CHARX SEC-3050
- Firmware < 1.6.3 installed on CHARX SEC-3100
- Firmware < 1.6.3 installed on CHARX SEC-3150

Fixed Products.

- Firmware 1.6.3 installed on CHARX SEC-3000
- Firmware 1.6.3 installed on CHARX SEC-3050
- Firmware 1.6.3 installed on CHARX SEC-3100
- Firmware 1.6.3 installed on CHARX SEC-3150

Vulnerabilities

CVE-2024-3913 (CVE-2024-3913)

Summary

An unauthenticated remote attacker can use this vulnerability to change the device configuration due to a file writeable for short time after system startup.

CWE:	CWE-552:Files or Directories Accessible to External Parties
Release date:	Tue Aug 13 12:00:00 CEST 2024

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 1.6.3 installed on CHARX SEC-3000 Order number(s): 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 1.6.3 installed on CHARX SEC-3050 Order number(s): 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 1.6.3 installed on CHARX SEC-3100 Order number(s): 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware < 1.6.3 installed on CHARX SEC-3150 Order number(s): 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product	CVSS-Vector	CVSS Base Score
Firmware 1.6.3 installed on CHARX SEC-3000 Order number(s): 1139022		
Firmware 1.6.3 installed on CHARX SEC-3050 Order number(s): 1139018		
Firmware 1.6.3 installed on CHARX SEC-3100 Order number(s): 1139012		
Firmware 1.6.3 installed on CHARX SEC-3150 Order number(s): 1138965		

Remediations

Vendor fix

Phoenix Contact strongly recommends upgrading affected charge controllers to firmware version 1.6.3 or higher which fixes these vulnerabilities.

For groups:

- Affected Products.

Workaround

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 General Recommendation.

For groups:

- Affected Products.

CVE-2024-6788 (CVE-2024-6788)

Summary

A remote unauthenticated attacker can use the firmware update feature on the LAN interface of the device to reset the password for the predefined, low-privileged user “user-app” to the default password.

CWE:	CWE-1188:Initialization of a Resource with an Insecure Default
Release date:	Tue Aug 13 12:00:00 CEST 2024

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 1.6.3 installed on CHARX SEC-3000 Order number(s): 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware < 1.6.3 installed on CHARX SEC-3050 Order number(s): 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware < 1.6.3 installed on CHARX SEC-3100 Order number(s): 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware < 1.6.3 installed on CHARX SEC-3150 Order number(s): 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6

Fixed

Product	CVSS-Vector	CVSS Base Score
Firmware 1.6.3 installed on CHARX SEC-3000 Order number(s): 1139022		
Firmware 1.6.3 installed on CHARX SEC-3050 Order number(s): 1139018		
Firmware 1.6.3 installed on CHARX SEC-3100 Order number(s): 1139012		
Firmware 1.6.3 installed on CHARX SEC-3150 Order number(s): 1138965		

Remediations

Vendor fix

Phoenix Contact strongly recommends upgrading affected charge controllers to firmware version 1.6.3 or higher which fixes these vulnerabilities.

For groups:

- Affected Products.

Workaround

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 General Recommendation.

For groups:

- Affected Products.

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERTVDE for coordination (see: https://certvde.com)
- Alex Olson, "gadha" from Trend Micro's Zero Day Initiative for reporting (see: https://www.zerodayinitiative.com/)
- McCaulay Hudson, Alexander Plaskett from NCC Group for reporting (see: https://www.nccgroup.com/)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2024/00003: (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://cert.vde.com/de/advisories/vendor/phoenixcontact/
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf
- VDE-2024-022: Phoenix Contact: Start sequence allows attack during the boot process (SELF): https://cert.vde.com/en/advisories/VDE-2024-022/

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Aug 13 12:00:00 CEST 2024	initial revision

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/