Bender GmbH & Co. KG

Bender Security Advisory BENDER-2021-001

Title

Multiple Charge Controller Vulnerabilities

Rating

high

Affected Products

- All Charge Controller product families are affected including CC612, CC613, ICC15xx and ICC16xx.
- The versions 5.11.x and 5.12.x are significantly affected, the versions 5.13.x and 5.20.x are partially affected by the weakness.

Summary

Bender is publishing this advisory to inform customers about multiple security vulnerabilities in the Charge Controller product families.
We have analysed the weaknesses and determined that the electrical safety of the devices is **not concerned**. To our knowledge, proof-of-concept code or exploits for the weaknesses are **not available** to the public.
Bender considers some weaknesses to be critical and thus need to be patched immediately. Therefore, patches are provided as maintenance branch versions 5.11.2, 5.12.5, 5.13.2 and 5.20.2. Future software releases will of course already include these patches.

Impact

The vulnerability allows a malicious entity to bypass credential check and escalate privileges

Mitigation

- restrict network access to the above-mentioned devices
- or install latest software update

Security Updates

Charging station Manufacturers or Operators with a registered account may download the patch from the webpage https://office.elinc.de/svn/ebee/XChange/Releases/ChargeStationModule/.
To register, regain access to an account or receive the patches on another way please contact sales@ebee.berlin.

Vulnerability Characterization and CVSSv3 Rating

Vulnerability	CWE-121 Stack-based Buffer Overflow
CVSS Score	5.3 (Medium)
CVSS Vector	3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CVE-ID	CVE-2021-34587
Title	Long URL could lead to webserver crash
Description	The URL is used as input of an sprintf to a stack variable

Vulnerability	CWE-425 Direct Request ('Forced Browsing')
CVSS Score	8.6 (High)
CVSS Vector	3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
CVE-ID	CVE-2021-34588
Title	Unprotected data export
Description	Backup export is protected via a random key. The key is set at user login. It is empty after reboot

Vulnerability	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
CVSS Score	7.4 (High)
CVSS Vector	3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
CVE-ID	CVE-2021-34589
Title	RFID leak
Description	The RFID of the last charge event can be read without authentication via the web interface

Vulnerability	CWE-79 Improper Neutralization of Input During Web Page Generation
CVSS Score	6.5 (Medium)
CVSS Vector	3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N
CVE-ID	CVE-2021-34590
Title	Cross-site Scripting
Description	An authenticated attacker could write HTML Code into configuration values. These values are not properly escaped when displayed

Vulnerability	CWE-250 Execution with Unnecessary Privileges
CVSS Score	7.8 (High)
CVSS Vector	3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-ID	CVE-2021-34591
Title	Local privilege Escalation
Description	An authenticated attacker could get root access via the suid applications socat, ip udhcpc and ifplugd

Vulnerability	CWE-77 Improper Neutralization of Special Elements used in a Command
CVSS Score	6.5 (Medium)
CVSS Vector	3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-ID	CVE-2021-34592
Title	Command injection via Web interface
Description	An authenticated attacker could enter shell commands into some input fields

Vulnerability	CWE-78 Command injection
CVSS Score	8.8 (High)
CVSS Vector	3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-ID	CVE-2021-34602
Title	Command injection via Web interface
Description	An authenticated attacker could enter shell commands into some input fields that are executed with root privileges

Vulnerability	CWE-259 Use of Hard-coded Password
CVSS Score	9.8 (High)
CVSS Vector	3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-ID	CVE-2021-34601
Title	Hardcoded Credentials in Charge Controller
Description	Bender charge controller CC612 in version 5.20.1 and below is prone to hardcoded ssh credentials. An attacker may use the password to gain administrative access to the web-UI

Acknowledgements

Bender thanks the IT security researchers at OpenSource Security GmbH for their thorough and in-depth work.
Bender would also like to thank Qianxin StarV Security Lab, China.
The issue was coordinated by CERT@VDE.