Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal

Title: Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal
Advisory ID: ZSL-2022-5709
Type: Local/Remote
Impact: Exposure of System Information, Exposure of Sensitive Information
Risk: (4/5)
Release Date: 30.06.2022

Summary

pCO sistema is the solution CAREL offers its customers for managing HVAC/R applications and systems. It consists of programmable controllers, user interfaces, gateways and communication interfaces, remote management systems to offer the OEMs working in HVAC/R a control system that is powerful yet flexible, can be easily interfaced to the more widely-used Building Management Systems, and can also be integrated into proprietary supervisory systems.

Description

The device suffers from an unauthenticated arbitrary file disclosure vulnerability. Input passed through the 'file' GET parameter through the 'logdownload.cgi' Bash script is not properly verified before being used to download log files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.

Vendor

CAREL INDUSTRIES S.p.A. - https://www.carel.com

Affected Version

Firmware: A2.1.0 - B2.1.0
Application Software: 2.15.4A
Software version: v16 13020200

Tested On

GNU/Linux 4.11.12 (armv7l)
thttpd/2.29

Vendor Status

[10.05.2022] Vulnerability discovered.
[27.05.2022] Vendor contacted.
[27.05.2022] Vendor responds creating request ID 00027344. Will come back soon with an answer.
[29.06.2022] No response from the vendor.
[30.06.2022] Public security advisory released.

PoC

carelpco_dir.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://packetstormsecurity.com/files/167684/
[2] https://exchange.xforce.ibmcloud.com/vulnerabilities/230273
[3] https://cxsecurity.com/issue/WLB-2022070011
[4] https://www.exploit-db.com/exploits/50986
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37122
[6] https://nvd.nist.gov/vuln/detail/CVE-2022-37122
[7] https://www.tenable.com/cve/CVE-2022-37122

Changelog

[30.06.2022] - Initial release
[01.06.2022] - Added reference [1]
[02.06.2022] - Added reference [2]
[20.07.2022] - Added reference [3]
[29.07.2022] - Added reference [4]
[01.09.2022] - Added reference [5], [6] and [7]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Rete mirabilia**
- **We Suggest**
- **Profiles**
- Site Meter