

Common Weakness Enumeration

CWE-284: Improper Access Control

Common Vulnerability Scoring System

Base Score: 9.9 - Overall Score: 9.2 - Vector:

AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H/E:F/RL:O/RC:C

Technical Details

When making a simple configuration update, such as changing the system language, the entire system configuration is updated, being passed from the browser to the embedded web server. An attacker with access to the maintainer account can proxy this request and update their own account permissions.

An attacker can toggle the permission "sidebar:view:/view/terminal":false to true to enable access to a root terminal on the underlying embedded Linux operating system.

Resolution

Carel fixed this vulnerability in version 1.9.0_Hotfix_20220930; please update to this version to address the vulnerability. **Note: Carel declined to have Mandiant verify/test their fix**.

Discovery Credits

• Patrick Hurd, Mandiant

Disclosure Timeline

- 29-Jun-2022 & 30-Jun-2022 Contacted Carel customer support emails to request a cybersecurity contact.
- 29-Jun-2022 & 30-Jun-2022 Automated response to email.
- 11-Jul-2022 Response from Carel requesting technical details.
- 12-Jul-2022 Technical report delivered to Carel.
- 19-Jul-2022 Carel confirms issue was known, proposes to meet in September to publicly disclose.

- 15-Sep-2022 Carel confirms a patch is ready to be released 30-Sep, requests Mandiant to share example disclosures.
- 19-Sep-2022 Mandiant provides sample disclosures.
- 06-Oct-2022 Carel requests recommendations on publishing a security bulletin.
- 07-Oct-2022 Mandiant provides a recommendation for bulletin structure.
- 21-Oct-2022 Mandiant requests an update from Carel.
- 27-Oct-2022 Carel agrees to share bulletin draft by wk45.
- 03-Nov-2022 Carel shares a draft bulletin with Mandiant
- 16-Nov-2022 Carel confirms bulletin has been published

References

- Carel Website
- Mitre CVE-2022-34827