Authenticated Command Injection in Hirschmann BAT-C2

Date: 2022-11-23
Version: 1.0
References: CVE-2022-40282[1]

Executive Summary

The web server of Hirschmann BAT-C2 through 09.12.01.00R01 is vulnerable to an authenticated command injection.

Details

The web server of Hirschmann BAT-C2 through 09.12.01.00R01 is vulnerable to an authenticated command injection. This allows an authenticated attacker to pass commands to the shell of the system because a parameter of the `FsCreateDir` Ajax function is not sufficiently sanitized.

The CVSS v3.1 severity of this vulnerability is 7.2 (High):
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Impact

Passing a command line to the shell of the system allows an attacker to execute binaries present in the firmware of the device with arbitrary arguments.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	BAT-C2	BAT-C2	09.12.01.00R01 or lower

Solution

Updates are available, which address the vulnerability. Customers are advised to update their product.

Brand	Product Line / Platform	Product	Version
Hirschmann	BAT-C2	BAT-C2	09.13.01.00R04 or higher

For Help or Feedback

To view all Belden Security Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com.

Acknowledgments

Belden thanks the following for working with us to help protect customers:

- Thomas Weber, CyberDanube Security Research

Related Links

- [1] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-40282

Disclaimer

Revisions

V1.0 (2022-11-23):	Bulletin published.