Talos Vulnerability Report

TALOS-2022-1470

InHand Networks InRouter302 web interface session cookie information disclosure vulnerability

MAY 10, 2022

CVE NUMBER

CVE-2022-25172

Summary

An information disclosure vulnerability exists in the web interface session cookie functionality of InHand Networks InRouter302 V3.5.4. The session cookie misses the HttpOnly flag, making it accessible via JavaScript and thus allowing an attacker, able to perform an XSS attack, to steal the session cookie.

Tested Versions

InHand Networks InRouter302 V3.5.4

Product URLs

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

CVSSv3 Score

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

CWE

CWE-1004 - Sensitive Cookie Without ‘HttpOnly’ Flag

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 has a web interface where the login is required to perform any actions. The login part is performed using JavaScript. Following the function that performs the login request:

```
function onOk()
{
    creatAjaxReq(
                "check_auth.jsp?_ajax=1&_username=" +
                escape(E('username').value) +
                "&_passwd=" +
                escape(E('passwd').value));
} The above function will call a custom function called `creatAjaxReq` that will
perform a GET request to the server to obtain a session cookie, if the credentials
provided are correct.
```

Then, if the credentials were correct, the `onSuccess` function will be called and the session cookie will be updated with the one provided by the server:

```
function onSuccess(txt) {
    var v = txt.split(',');
    if( v[0] == "OK" ){
        document.cookie = 'web_session=' + v[1] + '; expires=' +
            (new Date(new Date().getTime() + (1 * 86400000))).toUTCString() + ';
path=/';                [1]
        E('login_msg').innerHTML=txt_login_ok;
        page = "index.jsp";

        setTimeout(loadPage, 1000);
    }else{
       [...]
    }
}
```

At `[1]` the session cookie is set without the `HttpOnly` flag, which means that an attacker, able to inject arbitrary JavaScript in a page, would be able to steal the `web_session` cookie. This cookie can then be used to login to the web interface.

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

2022-02-25 - Initial vendor contact

2022-03-02 - Vendor Disclosure

2022-05-10 - Public Release

2022-05-10 - Vendor Patch Release

CREDIT

Discovered by Francesco Benvenuto of Cisco Talos.
