Talos Vulnerability Report

TALOS-2021-1360

Advantech R-SeeNet installation privilege escalation vulnerability

NOVEMBER 22, 2021

CVE NUMBER

CVE-2021-21910, CVE-2021-21911, CVE-2021-21912

Summary

A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021)

Product URLs

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

CVSSv3 Score

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

CWE

CWE-276 - Incorrect Default Permissions

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-2021-21910 - Privilege escalation via mysql service executable

By default, Advantech R-SeeNet is installed in the “C:\R-SeeNet" directory, which allows the “Authenticated Users” group to have “Full/Change” privilege over the “mysql” service binary file in the directory. These are executed with NT SYSTEM authority, leading to privilge escalation when the file is replaced and service is restarted.

```
C:\R-SeeNet\mysql\bin\mysqld.exe BUILTIN\Administrators:(ID)F
                                                          NT AUTHORITY\SYSTEM:(ID)F
                                                          BUILTIN\Users:(ID)R
                                                          NT AUTHORITY\Authenticated Users:(ID)C
```

CVE-2021-21911 - Privilege escalation via SnmpMonSvs service executable

By default, Advantech R-SeeNet is installed in the “C:\R-SeeNet" directory, which allows the “Authenticated Users” group to have “Full/Change” privilege over the “SnmpMonSvs” service binary file in the directory. These are executed with NT SYSTEM authority, leading to privilge escalation when the file is replaced and service is restarted.

```
C:\R-SeeNet\R_SeeNet.exe BUILTIN\Administrators:(ID)F
                                              NT AUTHORITY\SYSTEM:(ID)F
                                              BUILTIN\Users:(ID)R
                                              NT AUTHORITY\Authenticated Users:(ID)C
```

CVE-2021-21912 - Privilege escalation via Apache2.2 service executable

By default, Advantech R-SeeNet is installed in the “C:\R-SeeNet" directory, which allows the “Authenticated Users” group to have “Full/Change” privilege over “Apache2.2” service binary file in the directory. These are executed with NT SYSTEM authority,leading to privilge escalation when the file is replaced and service is restarted.

```
C:\R-SeeNet\apache\bin\httpd.exe BUILTIN\Administrators:(ID)F
                                                          NT AUTHORITY\SYSTEM:(ID)F
                                                          BUILTIN\Users:(ID)R
                                                          NT AUTHORITY\Authenticated Users:(ID)C
```

Timeline

2021-08-23 - Vendor Disclosure
2021-11-16 - Vendor Patched
2021-11-22 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.