SA-2021-03-01

ADVANTECH

Notification Date: November 19, 2021

SECURITY ADVISORY

R-SeeNet SQL Injection and Priviledge Escallation Vulnerabilities

Summary

Several security vulnerabilities of high severity have been discovered that affect R-SeeNet 2.4.16 and prior. Various specially crafted HTTP requests made by an authenticated user can lead to SQL injection. Also, in the Windows installation, a specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority.

Issue Description

1. TALOS-2021-1363: Advantech R-SeeNet application multiple SQL injection vulnerabilities in the 'group_list' page.
   Severity: Score 7.7 (High), CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
   Affected products: R-SeeNet 2.4.16 and prior, both Linux and Windows installations.
   Also known as: CVE-2021-21915, CVE-2021-21916, CVE-2021-21917

2. TALOS-2021-1364: Advantech R-SeeNet application multiple SQL injection vulnerabilities in the 'company_list' page.
   Severity: Score 7.7 (High), CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
   Affected products: R-SeeNet 2.4.16 and prior, both Linux and Windows installations.
   Also known as: CVE-2021-21918, CVE-2021-21919

3. TALOS-2021-1365: Advantech R-SeeNet application multiple SQL injection vulnerabilites in the 'user_list' page.
   Severity: Score 7.7 (High), CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
   Affected products: R-SeeNet 2.4.16 and prior, both Linux and Windows installations.
   Also known as: CVE-2021-21920, CVE-2021-21921, CVE-2021-21922, CVE-2021-21923

4. TALOS-2021-1366: Advantech R-SeeNet application multiple SQL injection vulnerabilites in the 'device_list' page.
   Severity: Score 7.7 (High), CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
   Affected products: R-SeeNet 2.4.16 and prior, both Linux and Windows installations.
   Also known as: CVE-2021-21924, CVE-2021-21925, CVE-2021-21926, CVE-2021-21927, CVE-2021-21928, CVE-2021-21929, CVE-2021-21930, CVE-2021-21931, CVE-2021-21932, CVE-2021-21933, CVE-2021-21934, CVE-2021-21935, CVE-2021-21936, CVE-2021-21937

5. TALOS-2021-1360: Advantech R-SeeNet installation privilege escalation vulnerability.
   Severity: Score 8.8 (High), CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
   Affected products: R-SeeNet 2.4.16 and prior, Windows installations only.
   Also known as: CVE-2021-21910, CVE-2021-21911, CVE-2021-21912

Solution

Users are recommended to upgrade to R-SeeNet 2.4.17.

Acknowledgement

These vulnerabilities have been discovered by Yuri Kramarz of Cisco Talos.

Related Advisories

ICSA-21-348-01

Revision History

2021-11-19 Advisory published
2021-12-15 Added a reference to the ICSA advisory