SA-2020-01-01

Notification Date: October 1, 2020

SECURITY ADVISORY

R-SeeNet Information Disclosure Vulnerability

Summary

Advantech R-SeeNet, versions 2.4.10 and prior, contain an SQL injection vulnerability, which allows remote attackers to retrieve sensitive information from the R-SeeNet database.

Issue Description

R-SeeNet versions 1.5.1–1.5.3 had a dedicated webpage to view a GPS position of a router. This was later modified to a direct invocation of Google maps, leaving the original implementation unused, but still included in all later versions through 2.4.10.

The device_position.php suffers from SQL Injection, which allows anyone connected to invoke SQL SELECT queries on the R-SeeNet database. No credentials are needed. This can be used e.g. to retrieve the hashes of user passwords or the ICMP community strings of the individual routers.

This impacts confidentiality of the information stored in the R-SeeNet database. It is not possible though to use this vulnerability for invoking other SQL queries such as UPDATE, so integrity and availability is not impacted.

A known approach how to exploit this vulnerability needs a higher amount of HTTP requests to retrieve the information. Hence, the HTTP server log monitoring might be able to capture this attack.

Severity

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Score 7.5 (High)

Affected Products

R-SeeNet 1.5.1 through 2.4.10 is affected, both Linux and Windows versions.

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661

Workaround

Simply delete the `C:\R-SeeNet\php\device\_position.php` (on Windows)
or `/usr/share/r-seenet/www/php/php/device\_position.php` (on Linux)

This fully addresses this vulnerability and does not degrade any functionality, because the file is not used since R-SeeNet 1.5.3.

Solution

Users are recommended to upgrade to R-SeeNet 2.4.11

Acknowledgement

This vulnerability was discovered by rgod working with Trend Micro Zero Day Initiative.

Related Advisories

CVE-2020-25157
ZDI-CAN-11373
ZDI-20-1262
ICSA-20-289-02

Revision History

2020-10-01 Advisory published
2020-10-23 Added references to CVE, ZDI and ICSA advisories

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661