



CVE-2021-21800

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-21800
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-16 11:15:00 UTC
Updated	2022-09-30 03:08:00 UTC
Description	Cross-site scripting vulnerabilities exist in the ssh_form.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020)

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	R-seenet	2.4.12	All	All	All

References

Reference	Source	Link	Tags
TALOS-2021-1271 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730219](#) Advantech R-SeeNet ssh_form.php Reflected Cross-Site Scripting (XSS) Vulnerability

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)