



CVE-2020-35437

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

Summary

CVE	CVE-2020-35437
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-26 04:15:00 UTC
Updated	2022-07-17 12:47:00 UTC
Description	Subrion CMS 4.2.1 is affected by: Cross Site Scripting (XSS) through the avatar[path] parameter in a POST request to the /

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intelliants	Subrion Cms	4.2.1	All	All	All
Application	Intelliants	Subrion Cms	4.2.1	All	All	All

References

Reference	Source	Link	Tags
/_core/profile/ stored xss vulnerability · Issue #880 · intelliants/subrion · GitHub	MISC	github.com	Exploit, Third Party
Subrion CMS 4.2.1 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report