CVE-2021-22872

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-22872
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:16:00 UTC
Updated	2021-02-02 19:59:00 UTC
Description	Revive Adserver before 5.1.0 is vulnerable to a reflected cross-site scripting (XSS) vulnerability via the publicly accessible a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Revive-adserver	Revive Adserver	All	All	All	All
Application	Revive-adserver	Revive Adserver	All	All	All	All

References

Reference	Source	Link	Tags
HackerOne	MISC	hackerone.com	Exploit, Third P
Full Disclosure: [REVIVE-SA-2021-001] Revive Adserver Vulnerabilities	FULLDISC	seclists.org	Broken Link, M
Revive Adserver 5.0.5 Cross Site Scripting / Open Redirect ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Adv
Regenerated delivery scripts · revive-adserver/revive-adserver@1dbcf7d · GitHub	MISC	github.com	Patch, Third Pa
Fix h1 report 986365 · revive-adserver/revive-adserver@00fdb8d · GitHub	MISC	github.com	Patch, Third Pa
Revive Adserver Security Advisory SA-2021-001	MISC	www.revive-adserver.com	Vendor Advisor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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