



CVE-2016-9126

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

Summary

CVE	CVE-2016-9126
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-28 02:59:00 UTC
Updated	2019-10-09 23:20:00 UTC
Description	Revive Adserver before 3.2.3 suffers from persistent XSS. Usernames are not properly escaped when displayed in the audi

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

References

Reference	Source	Link	Tags
Revive Adserver Security Advisory SA-2016-001 Revive Adserver	MISC	www.revive-adserver.com	Patch, Vendor Advisory
HackerOne	MISC	hackerone.com	Permissions Required
Fix h1 report 97073 · revive-adserver/revive-adserver@8d8c6df · GitHub	MISC	github.com	Issue Tracking, Patch, T
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