



CVE-2020-8115

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

Summary

CVE	CVE-2020-8115
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-04 20:15:00 UTC
Updated	2020-02-11 13:40:00 UTC
Description	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.

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-2020-001	MISC	www.revive-adserver.com	Vendor Advisory
HackerOne	MISC	hackerone.com	Exploit, Patch, Third Party Advisory
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.

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