



CVE-2021-22873

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

Summary

CVE	CVE-2021-22873
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 15:09:00 UTC
Description	Revive Adserver before 5.1.0 is vulnerable to open redirects via the `dest`, `oadest`, and/or `ct0` parameters of the lg.php a

Risk And Classification

Problem Types: CWE-601

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
HackerOne	MISC	hackerone.com
open redirect (oadest url) ck.php revive 4.2.1 · Issue #1068 · revive-adserver/revive-adserver · GitHub	MISC	github.com
Full Disclosure: [REVIVE-SA-2021-001] Revive Adserver Vulnerabilities	FULLDISC	seclists.org
Revive Adserver 5.0.5 Cross Site Scripting / Open Redirect ≈ Packet Storm	MISC	packetstormsecurity.com
Revive Adserver Security Advisory SA-2021-001	MISC	www.revive-adserver.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)