



CVE-2023-32761

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

Summary

CVE	CVE-2023-32761
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-14 18:15:00 UTC
Updated	2023-07-27 14:29:00 UTC
Description	Cross Site Request Forgery (CSRF) vulnerability in Archer Platform before v.6.13 and fixed in v.6.12.0.6 and v.6.13.0 allow

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Archerirm	Archer	All	All	All	All

References

Reference	Source	Link	Tags
Archer Announces Availability of Archer Release 6.13 - Archer Community - 697821	MISC	www.archerirm.community	
Archer Update for Multiple Vulnerabilities - Archer Community - 702362	CONFIRM	www.archerirm.community	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

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