



CVE-2023-20856

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

Summary

CVE	CVE-2023-20856
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-01 03:15:00 UTC
Updated	2023-02-08 02:34:00 UTC
Description	VMware vRealize Operations (vROps) contains a CSRF bypass vulnerability. A malicious user could execute actions on the

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Vrealize Operations	All	All	All	All

References

Reference	Source	Link	Tags
VMSA-2023-0002	MISC	www.vmware.com	
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.

Legacy QID Mappings

[377961](#) VMware vRealize Operations (vROps) CSRF Bypass Vulnerability (VMSA-2023-0002)

[730722](#) VMware vRealize Operations (vROps) Cross-Site Request Forgery (CSRF) Bypass Vulnerability (VMSA-2023-0002)

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