



CVE-2023-20888

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-20888
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-07 15:15:00 UTC
Updated	2023-06-14 19:10:00 UTC
Description	Aria Operations for Networks contains an authenticated deserialization vulnerability. A malicious actor with network access

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Vrealize Network Insight	All	All	All	All

References

Reference	Source	Link	Tags
VMSA-2023-0012	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

[378558](#) VMware Aria Operations for Networks Multiple Security Vulnerabilities (VMSA-2023-0012)

[730825](#) VMware Aria Operations for Networks Multiple Security Vulnerabilities (VMSA-2023-0012.1)

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