

VMware Aria Operations for Networks Command Injection Vulnerability

Actively exploited in the wild

<https://www.vmware.com/security/advisories/VMSA-2023-0012.html>
 CVEs: CVE-2023-20887

VMware Aria Operations for Networks (formerly vRealize Network Insight) contains a command injection vulnerability that allows a malicious actor with network access to perform an attack resulting in remote code execution. According to the vendor advisory, the vulnerability has been seen exploited in the wild.

Background VMware Aria Operations for Networks is a network monitoring tool that helps to build an optimized, highly available and secure network infrastructure across multicloud environments. It consists both SaaS and on-premises solutions. Early June, 2023, VMware Aria Operations for Networks update was released which addressed multiple vulnerabilities. (CVE-2023-20887, CVE-2023-20888, CVE-2023-20889). VMware has confirmed that exploit code (proof-of-concept) for CVE-2023-20887 is available online.

Announced June 7, 2023: VMware Aria Operations for Networks released security advisory. <https://www.vmware.com/security/advisories/VMSA-2023-0012.html>

June 20, 2023: VMware confirmed that exploitation of CVE-2023-20887 has occurred in the wild.

Latest Developments June 22, 2023: CISA added CVE-2023-20887 to its known exploited vulnerability catalog (KEV).

June 22, 2023: FortiGuard Labs has released the IPS signature to block any attack attempts targeting the vulnerability (CVE-2023-20887). To remediate risk completely, apply the updates listed on the vendor links provided.

<https://kb.vmware.com/s/article/92684>

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance


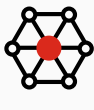

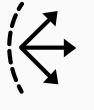

Weaponization

Delivery

Exploitation



IPS

Detects and Blocks attack attempts targeting vulnerable VMware Aria Operations (CVE-2023-20887)

 FortiGate DB 24.588	 FortiSASE DB 24.588	 FortiNDR DB 24.588	 FortiADC DB 24.588	 FortiProxy DB 24.588
---	---	--	--	--

Web App Security


Detects and Blocks attack attempts targeting vulnerable VMware Aria Operations (CVE-2023-20887)

 FortiWeb DB 0.00353	 FortiADC DB 1.00043
---	---

Installation

Post-execution

Detects and Blocks post exploitation activity related to unknown and 0-day malware

 FortiEDR v4.0+
--




C2

Action


DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:


Threat Hunting

 FortiEDR v4.0+	 FortiAnalyzer v6.4+	 FortiSIEM v6.5+
--	---	---

Outbreak Detection

 FortiAnalyzer DB 2.00009
--

Content Update

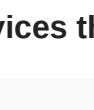
 FortiSIEM DB 409
--

RESPOND

Develop containment techniques to mitigate impacts of security events:



Automated Response

Services that can automatically respond to this outbreak.

 FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.


 Incident Response	 FortiRecon: ACI
--	--

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

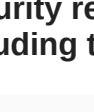
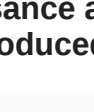
 Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

 Security Rating	 FortiRecon: EASM
--	---

Additional Resources

- FortiGuard Threat Signal <https://www.fortiguard.com/threat-signal-report/5202>
- Bleeping Computer <https://www.bleepingcomputer.com/news/security/vmware-warns-of-critical-vrealize-flaw-exploited-in-attacks/>
- CISA KEV <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- The Hacker News <https://thehackernews.com/2023/06/alert-hackers-exploiting-critical.html>

Learn more about [FortiGuard Outbreak Alerts](#)