



Zoho ManageEngine RCE Vulnerability

Multiple Zoho ManageEngine products exploited in the wild

<https://www.manageengine.com/security/advisory/CVE-2022-47966.html>
 CVEs: CVE-2022-47966

Multiple Zoho ManageEngine on-premise products, such as ServiceDesk Plus, Password Manager Pro and ADSelfService Plus, allow remote code execution due to the usage of an outdated third party dependency, Apache Santuario. Successful exploitation could lead to remote code execution and evidence of exploitation in the wild by Advanced Persistent Threat (APT) Groups.

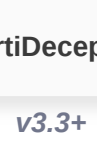
Background	ManageEngine's products are widely used across enterprises with broad suite of IT management software which perform several important business functions. Previously in 2021, we saw a different vulnerability, Zoho ManageEngine ServiceDesk Plus (CVE-2021-44077) exploited in the wild. Full Outbreak Report can be read here: https://www.fortiguard.com/outbreak-alert/zoho-exploit
Announced	Jan 20, 2023: FortiGuard Labs released a Threat Signal Report on Proof-of-Concept Released for Zoho ManageEngine RCE vulnerability (CVE-2022-47966). https://www.fortiguard.com/threat-signal-report/4954/
	Jan 23,2023: FortiGuard Labs released an IPS signature (ID: 52571) to detect and block any attack attempts targeting CVE-2022-47966.
Latest Developments	Jan 23, 2023: CISA added CVE-2022-47966 to its Known Exploited Vulnerabilities Catalog (KEV) https://www.cisa.gov/known-exploited-vulnerabilities-catalog
	April 18, 2023: Microsoft Threat Intelligence linked Mint Sandstorm, an Iranian government-backed threat actor to exploit Zoho ManageEngine vulnerability to gain initial access and targeting of US critical infrastructure. https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/
	FortiGuard Labs recommends organizations using any of the affected products listed in ManageEngine's advisory to update immediately as exploit code is publicly available and exploitation is in the wild.

PROTECT

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

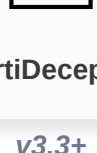
Reconnaissance

Lure



FortiDeceptor
v3.3+

Decoy VM



FortiDeceptor
v3.3+

Weaponization

Delivery

AV

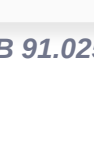
Detects and blocks known malware related to Zoho ManageEngine RCE campaign (CVE-2022-47966)



FortiGate
DB 91.02544



FortiWeb
DB 91.02544



FortiClient
DB 91.02544



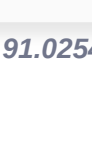
FortiSASE
DB 91.02544



FortiMail
DB 91.02544



FortiCASB
DB 91.02544



FortiCWP
DB 91.02544



FortiADC
DB 91.02544



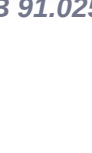
FortiProxy
DB 91.02544

AV (Pre-filter)

Detects and blocks known malware related to Zoho ManageEngine RCE campaign (CVE-2022-47966)



FortiEDR
DB 91.02544



FortiSandbox
DB 91.02544



FortiNDR
DB 91.02544

Exploitation

IPS

Detects and blocks attack attempts related to Zoho ManageEngine RCE Vulnerability (CVE-2022-47966)



FortiGate
DB 23.536



FortiSASE
DB 23.536



FortiNDR
DB 23.536



FortiADC
DB 23.536



FortiProxy
DB 23.536

Web App Security

Detects and blocks attack attempts related to Zoho ManageEngine RCE Vulnerability (CVE-2022-47966)



FortiWeb
DB 0.00342



FortiADC
DB 1.00042

Installation

Post-execution

Detect and blocks post-exploitation activity associated with exploitation of CVE-2022-47966 and unkown threats



FortiEDR
v5.0+

C2

Botnet C&C

Blocks known C2 servers related to Zoho ManageEngine RCE campagin (CVE-2022-47966)



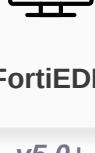
FortiGate
DB 3.00257

Action

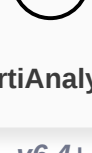
DETECT

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

Threat Hunting



FortiEDR
v5.0+

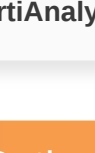


FortiAnalyzer
v6.4+

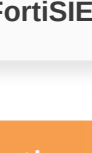


FortiSIEM
v6.6+

IOC



FortiAnalyzer



FortiSIEM



FortiSOCaaS

Outbreak Detection



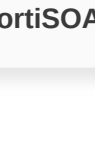
FortiAnalyzer
DB 1.00099

Content Update



FortiSIEM
DB 314

Playbook



FortiSOAR

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/4954
Helpnet Security	https://www.helpnetsecurity.com/2023/01/17/cve-2022-47966-poc/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/cisa-warns-of-critical-manageengine-rce-bug-exploited-in-attacks/
The Hacker News	https://thehackernews.com/2023/02/experts-sound-alarm-over-growing.html
Updated	2024-05-04 16:03:06

Learn more about [FortiGuard Outbreak Alerts](#)

