FORTINET

OUTBREAK ALERTS

VMware Workspace ONE Attack

Multiple malware campaigns targeting VMware vulnerability

https://www.fortinet.com/blog/threat-research/multiple-malware-campaigns-target-vmware-vulnerability
CVEs: CVE-2022-22954

Fortinet researchers observed VMware vulnerability (CVE-2022-22954) being exploited in the wild and leveraged to deliver multiple malware payloads such as cryptocurrency miners and ransomware on the affected machines. During August 2022, more than 50,000 devices were seen in attack attempts trying to exploit this vulnerability.

Background

VMware published a security advisory on April 2022 a CVE-2022-22954 vulnerability on their products VMware Workspace ONE Access, Identity Manager and vRealize Automation. A week later, VMware updated their advisory that CVE-2022-22954 is being exploited in the wild.
https://www.vmware.com/security/advisories/VMSA-2022-0011.html

Announced

In April, 2022, Fortiguard labs added protections throughout the Security Fabric to block any attack attempts and are actively monitoring ever evolving malware distribution leveraging the VMware vulnerability CVE-2022-22954. User are advised to patch vulnerable versions as per the vendor's recommendations.

Latest Developments

October 20, 2022, Fortinet researcher posted a blog elaborating exploitation of the VMware vulnerability and installation of the malware.
https://www.fortinet.com/blog/threat-research/multiple-malware-campaigns-target-vmware-vulnerability

PROTECT

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

- Reconnaissance
- Weaponization
- Delivery

AV

Block attack attempts related to VMware vulnerability (CVE-2022-22954)

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 90.07195	DB 90.07195	DB 90.07195	DB 90.07195	DB 90.07195	DB 90.07195	DB 90.07195

FortiADC	FortiProxy
DB 90.07195	DB 90.07195

AV (Pre-filter)

Block attack attempts related to VMware vulnerability (CVE-2022-22954)

FortiEDR	FortiSandbox	FortiNDR
DB 90.07195	DB 90.07195	DB 90.07195

- Exploitation

IPS

Block attack attempts related to VMware vulnerability (CVE-2022-22954)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 20.297	DB 20.297	DB 20.297	DB 20.297	DB 20.297

Web App Security

Block attack attempts related to VMware vulnerability (CVE-2022-22954)

FortiWeb	FortiADC
DB 0.00324	DB 1.00041

- Installation
- C2
- Action

DETECT

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

IOC

FortiAnalyzer	FortiSIEM	FortiSOCaaS
DB 0.02360	DB 0.02360	DB 0.02360

Outbreak Detection

FortiAnalyzer
DB 1.00073

Content Update

FortiSIEM
v6.6+

Threat Hunting

FortiSIEM
DB 309

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

Fortinet Blog	https://www.fortinet.com/blog/threat-research/multiple-malware-campaigns-target-vmware-vulnerability
Threat Singal	https://www.fortiguard.com/threat-signal-report/4496
VMware	https://kb.vmware.com/s/article/88099
Bleeping Computer	https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-vmware-flaw-to-drop-ransomware-miners/
The Hacker News	https://thehackernews.com/2022/10/multiple-campaigns-exploit-vmware.html

Learn more about FortiGuard Outbreak Alerts