



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/MSA-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:

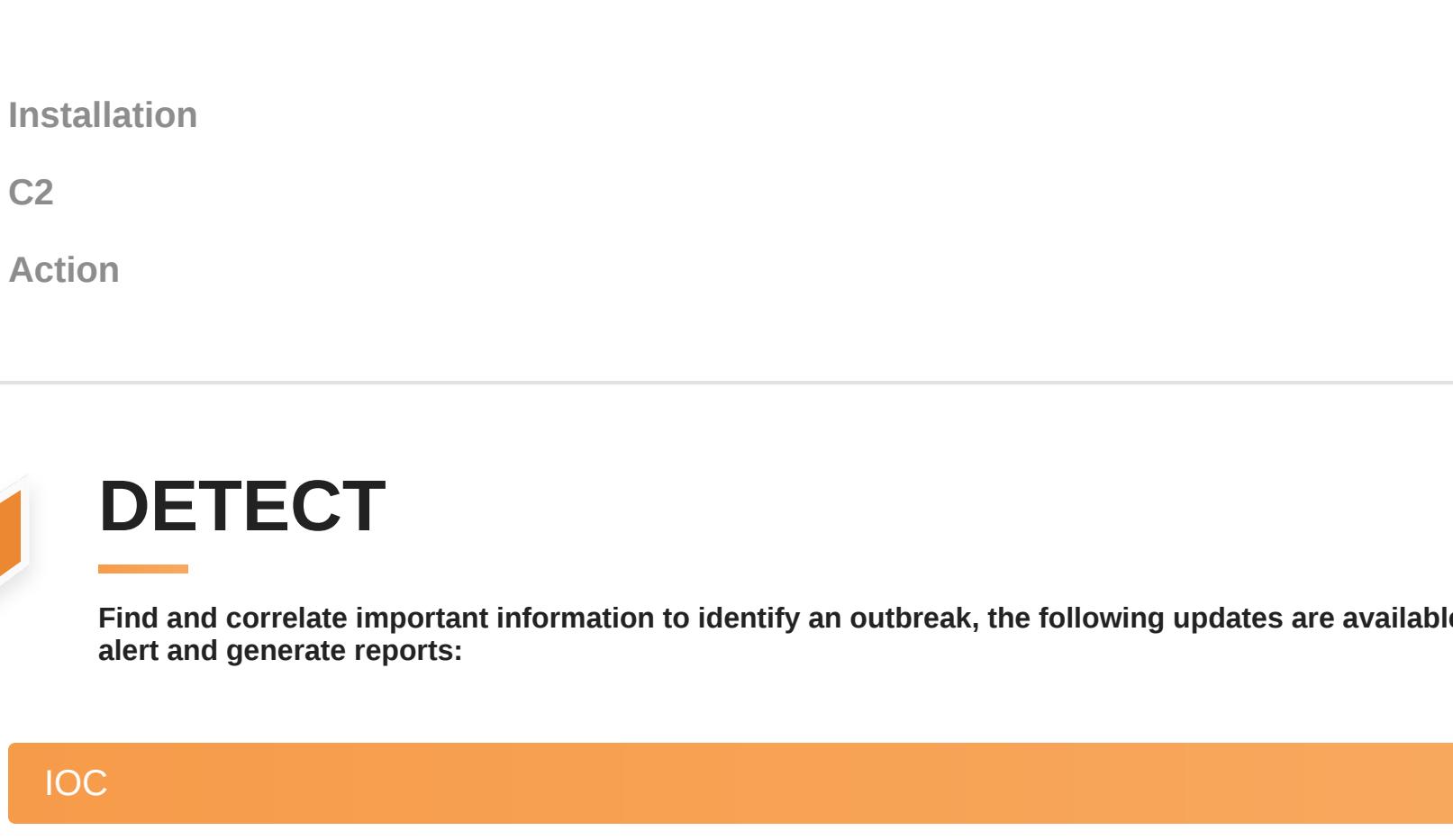
Reconnaissance

Weaponization

Delivery

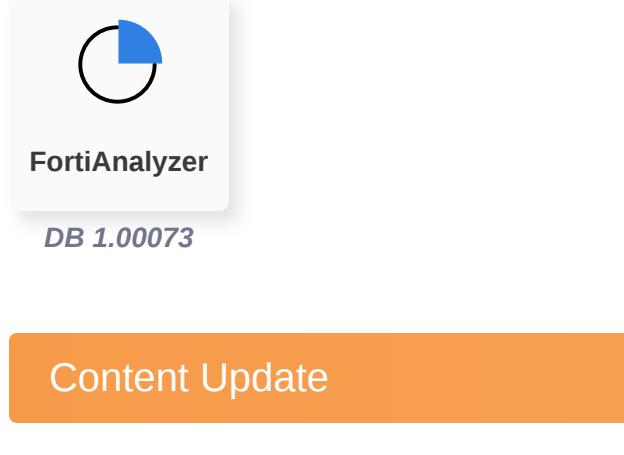
AV

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



AV (Pre-filter)

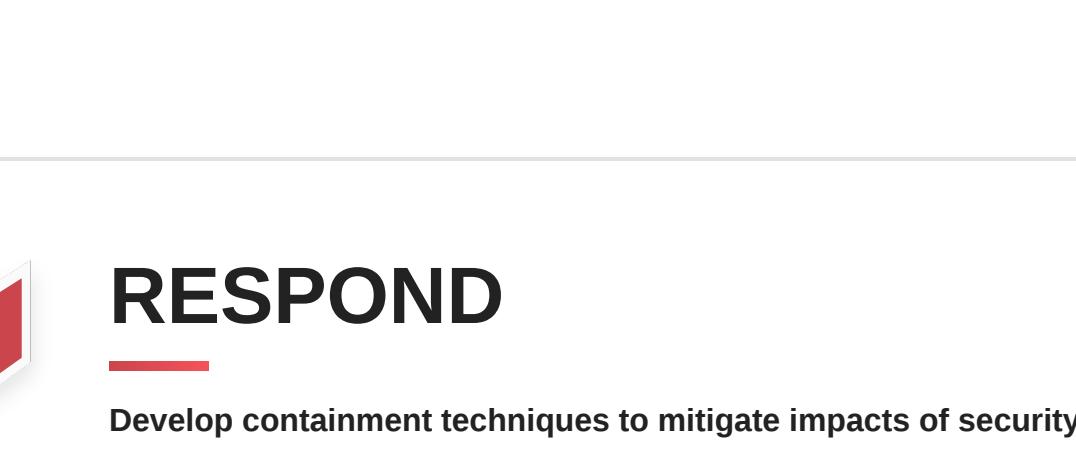
Block attack attempts related to VMware vulnerability (CVE-2022-22954)



Exploitation

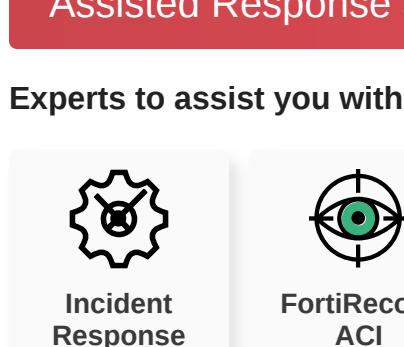
IPS

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



Web App Security

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



Installation

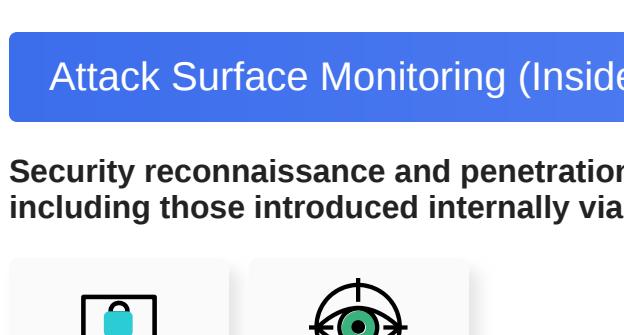
C2

Action

DETECT

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

IOC



Outbreak Detection



Content Update



Threat Hunting



RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

Assisted Response Services

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.

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:

Additional Resources

Fortinet Blog

<https://www.fortinet.com/blog/threat-research/multiple-malware-campaigns-target-vmware-vulnerability>

Threat Signal

<https://www.fortinet.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](#)

