

VMware ESXi Server Ransomware Attack

Ransomware targeting VMware ESXi OpenSLP vulnerability

<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/>

CVEs: CVE-2021-21974, CVE-2020-3992

ESXi servers vulnerable to the OpenSLP heap-overflow vulnerability (CVE-2021-21974) and OpenSLP remote code execution vulnerability (CVE-2020-3992) are being exploited through the OpenSLP, port 427 to deliver a new ransomware "ESXiArgs". The ransomware encrypts files in affected ESXi servers and demand a ransom for file decryption.

Background October 20, 2020: VMware released a patch and advisory for CVE-2020-3992.
<https://www.vmware.com/security/advisories/VMSA-2020-0023.html>

February 23, 2021: VMware released a patch and advisory for CVE-2021-21974.
<https://www.vmware.com/security/advisories/VMSA-2021-0002.html>

Announced February 03, 2023: CERT-FR posted an advisory for attack campaigns targeting vulnerable and unpatched VMware ESXi hypervisors with the aim of deploying ransomware.
<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/>

Latest Developments FortiGuard Labs is aware of exploitation reported in the wild. Fortinet's customer remain protected by the IPS signatures released to detect and block any attack attempts related to the vulnerability (CVE-2021-21974, CVE-2020-3992) and has recently added Antivirus detections to block "ESXiArgs" ransomware attacks.

The attack is primarily targeting ESXi servers in version before 7.0 U3i, through the OpenSLP port (427). To check your version of ESXi, please refer to your server page in your customer interface and steps to disable SLP service.
<https://kb.vmware.com/s/article/7637>

February 07, 2023: CISA Releases ESXiArgs Ransomware Recovery Script.
<https://www.cisa.gov/uscert/ncas/current-activity/2023/02/07/cisa-releases-esxiargs-ransomware-recovery-script>

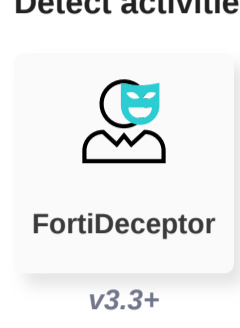
PROTECT

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

Reconnaissance

Decoy VM

Detect activities related to a ESXiArgs Ransomware Malware and prevents lateral movement on the network

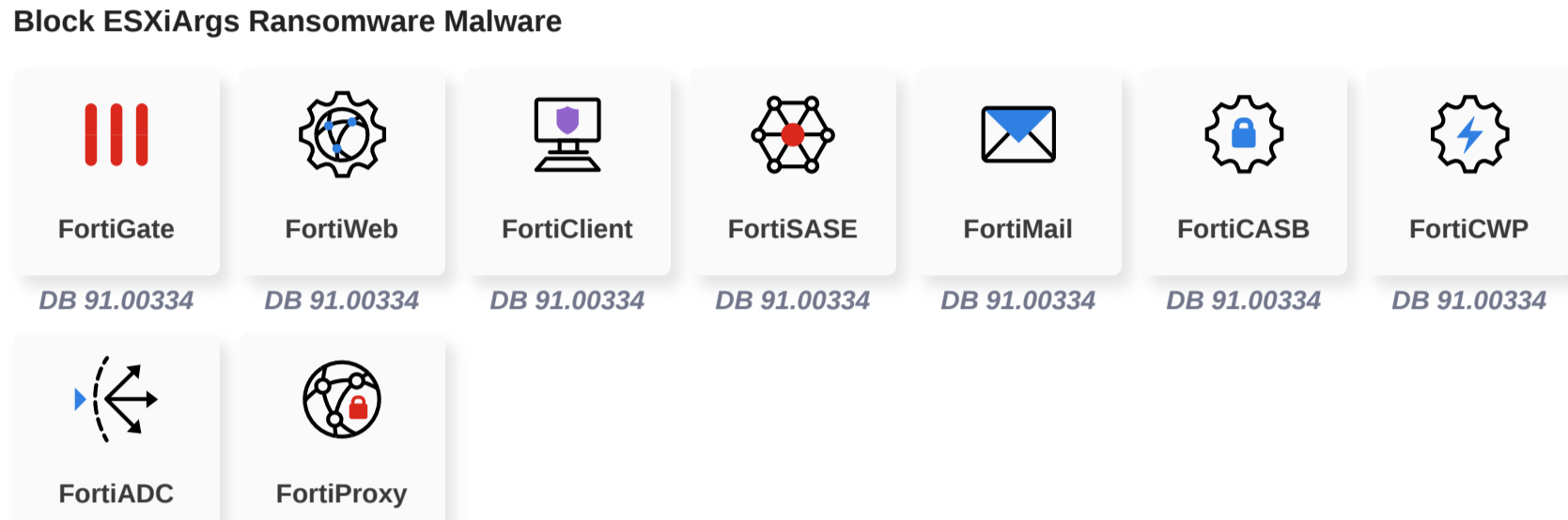


Weaponization

Delivery

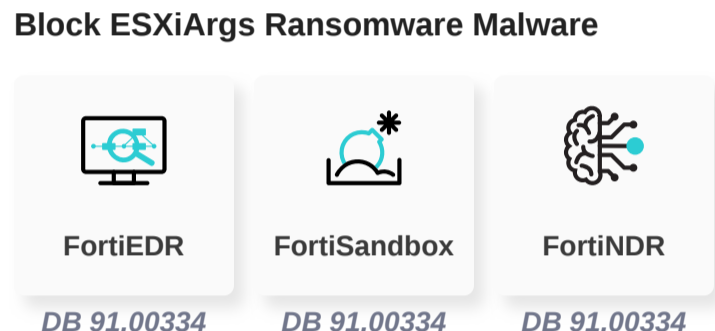
AV

Block ESXiArgs Ransomware Malware



AV (Pre-filter)

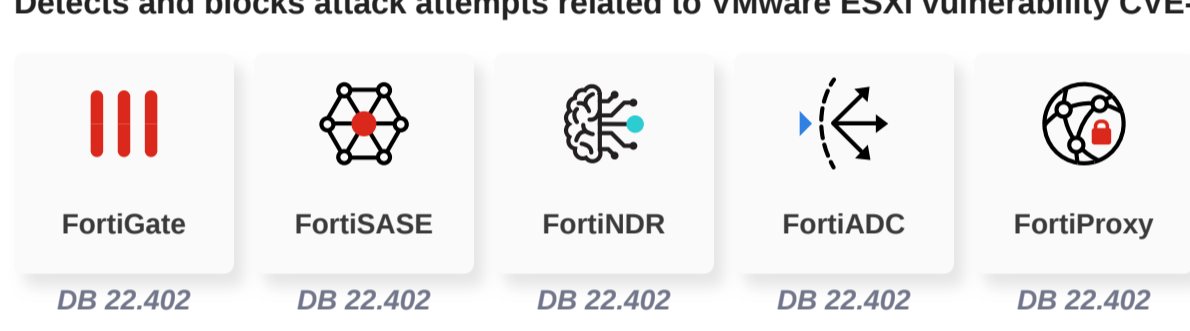
Block ESXiArgs Ransomware Malware



Exploitation

IPS

Detects and blocks attack attempts related to VMware ESXi vulnerability CVE-2021-21974.



Installation

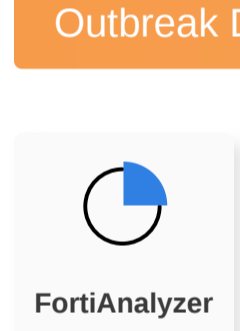
C2

Action

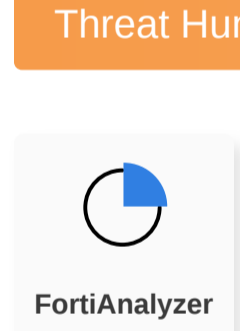
DETECT

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

Outbreak Detection



Threat Hunting

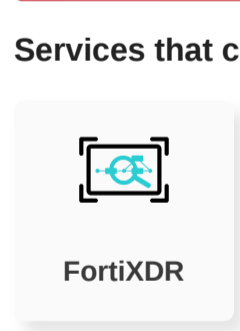


RESPOND

Develop containment techniques to mitigate impacts of security events:

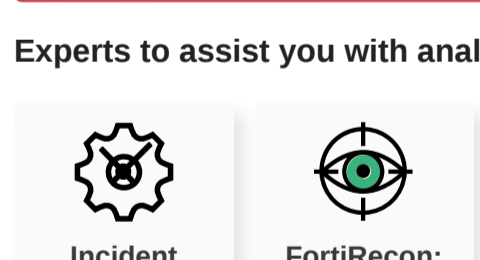
Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

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

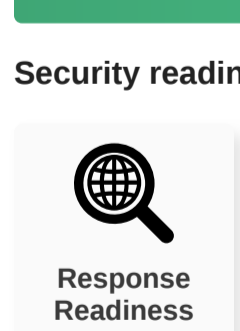


RECOVER

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.

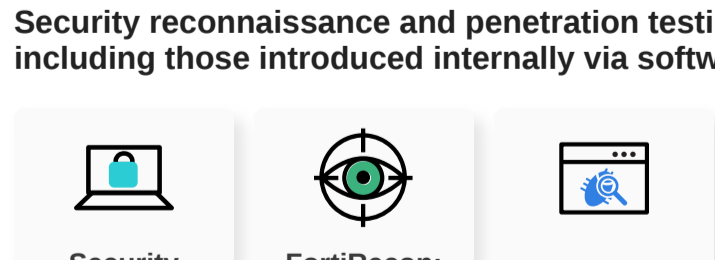


IDENTIFY

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 those introduced internally via software supply chain.



Additional Resources

Threat Signal	https://www.fortiguard.com/threat-signal-report/4988/
CERT-FR	https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
CSIRT-ITA	https://www.csirt.gov.it/contenuti/nilevato-lo-sfruttamento-massivo-della-cve-202121974-in-vmware-esxi-a01-230204-csirt-ita
VMware	https://www.vmware.com/security/advisories/VMSA-2021-0002.html
Helpnet Security	https://www.helpnetsecurity.com/2023/02/06/vmware-esxi-ransomware-cve-2021-21974/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
The Stack	https://thestack.technology/mass-esxi-ransomware-attacks-cve-2021-21974/

Learn more about [FortiGuard Outbreak Alerts](#)