

Microsoft Exchange ProxyNotShell Vulnerabilities

Zero-Day on Exchange Server Autodiscover actively being exploited in the wild

<https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/>
 CVEs: CVE-2022-41040, CVE-2022-41082, CVE-2022-41080

Critical zero-day vulnerabilities that can allow the attacker to do a Remote Code Execution (RCE) on Microsoft Exchange Servers. FortiGuard has added multiple protections throughout the Security Fabric to safeguard its customers from attacks exploiting these zero-day vulnerabilities.

Background A security researcher from a Vietnamese cybersecurity outfit GTSC spotted vulnerabilities on Microsoft Exchange Server while responding to an incident. The vulnerabilities have been reported three weeks ago through the Zero Day Initiative, which tracks them as ZDI-CAN-18333 and ZDI-CAN-18802.

Announced September 29, 2022: Security News picked up the blog from GTSC and announced the active exploitation of the Microsoft Exchange Server.

Latest Developments September 29, 2022: Multiple reports of exploitation in the wild leveraging the Microsoft Exchange Autodiscover 0-day vulnerabilities.
 September 29, 2022: Microsoft Security Response Center added customer guidance on their blog: <https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server>

PROTECT

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

Reconnaissance

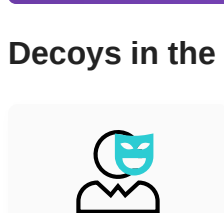
Lure

Deception Lure will divert attacker and its activities related to Microsoft Exchange ProxyNotShell Vulnerabilities towards FortiDeceptor Decoy



Decoy VM

Decoys in the Microsoft Exchange segment can detect the attack and any lateral movement.

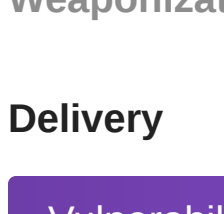


Weaponization

Delivery

Vulnerability

Detects endpoints vulnerable to Microsoft Exchange ProxyNotShell Vulnerabilities



Exploitation

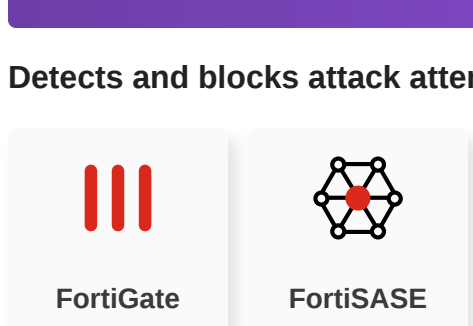
IPS

Detects and blocks attack attempts related to Microsoft Exchange ProxyNotShell Vulnerabilities



Web App Security

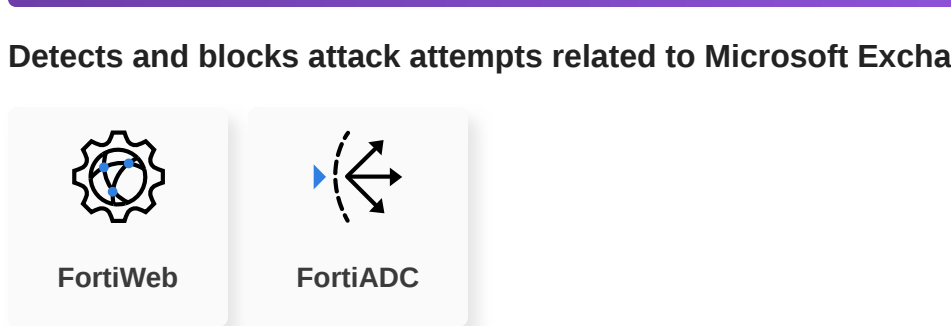
Detects and blocks attack attempts related to Microsoft Exchange ProxyNotShell Vulnerabilities



Installation

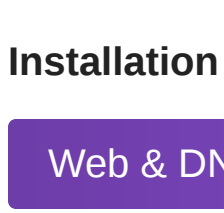
Web & DNS Filter

Detects published URL indicator (IOC) as malicious



Post-execution

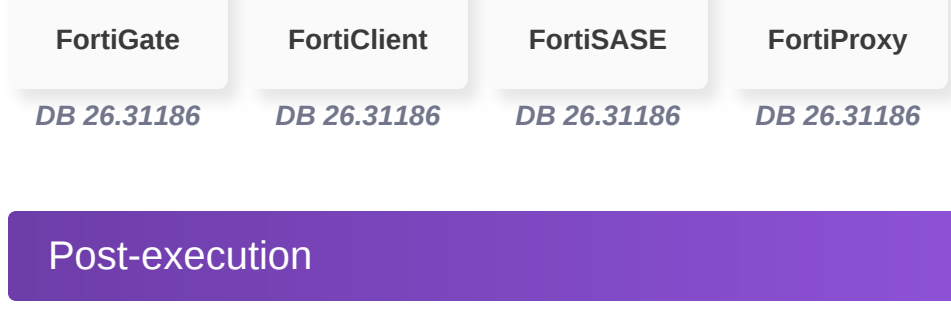
Delivers real-time visibility, analysis, protection and remediation for unknown threats and post exploitation activity.



C2

Botnet C&C

Detects published C2 indicator (IOC) as malicious

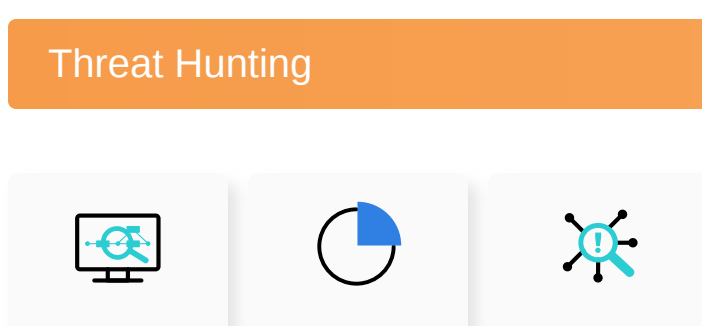


Action

DETECT

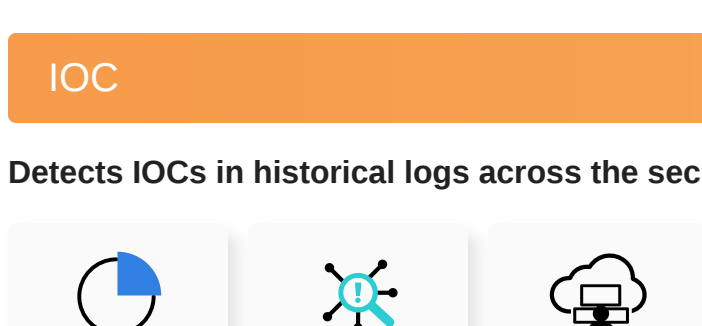
Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Threat Hunting



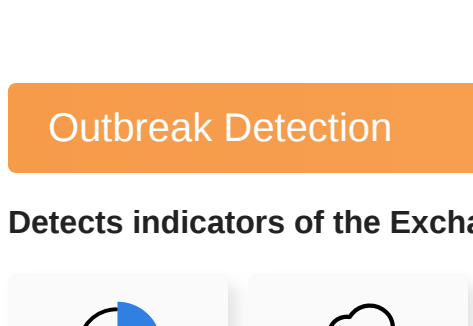
IOC

Detects IOCs in historical logs across the security fabric



Outbreak Detection

Detects indicators of the Exchange ProxyNotShell incident across the security fabric



Content Update

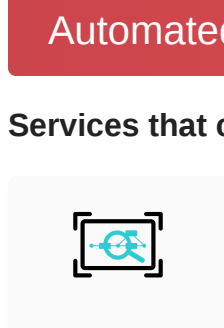


RESPOND

Develop containment techniques to mitigate impacts of security events:

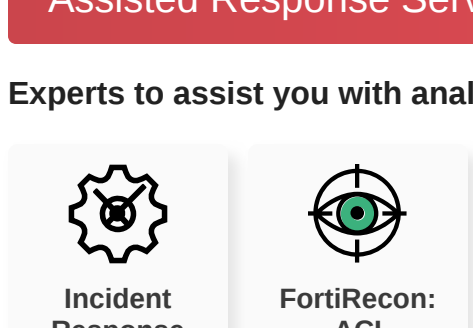
Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

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

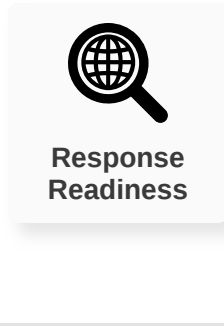


RECOVER

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.

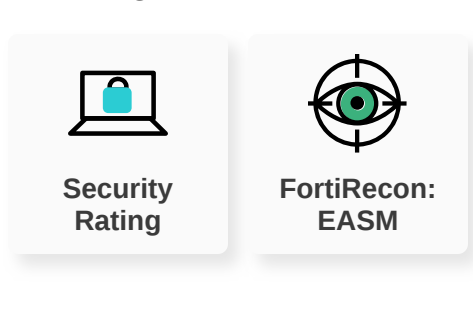


IDENTIFY

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

- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-day-actively-exploited-in-attacks/>
- GTSC** <https://www.gtstsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html>
- ZDI** <https://www.zerodayinitiative.com/advisories/upcoming>
- Threat Signal** <https://www.fortiguard.com/threat-signal-report/4779/possible-new-microsoft-exchange-rce-0-day-being-exploited-in-the-wild>
- Security Week** <https://www.securityweek.com/microsoft-confirms-exploitation-two-exchange-server-zero-days>

Learn more about [FortiGuard Outbreak Alerts](#)