FORTINET

OUTBREAK ALERTS

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

FortiDeceptor
v3.0+

Decoy VM

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

FortiDeceptor
v3.0+

Weaponization

Delivery

Vulnerability

Detects endpoints vulnerable to Microsoft Exchange ProxyNotShell Vulnerabilities

FortiClient
DB 1.354

Exploitation

IPS

Detects and blocks attack attempts related to Microsoft Exchange ProxyNotShell Vulnerabilities

FortiGate *DB 18.119* | FortiSASE *DB 18.119* | FortiNDR *DB 18.119* | FortiADC *DB 18.119* | FortiProxy *DB 18.119*

Web App Security

Detects and blocks attack attempts related to Microsoft Exchange ProxyNotShell Vulnerabilities

FortiWeb *DB 0.00315* | FortiADC *DB 1.00041*

Installation

Web & DNS Filter

Detects published URL indicator (IOC) as malicious

FortiGate *DB 26.31186* | FortiClient *DB 26.31186* | FortiSASE *DB 26.31186* | FortiProxy *DB 26.31186*

Post-execution

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

FortiEDR
v4.0+

C2

Botnet C&C

Detects published C2 indicator (IOC) as malicious

FortiGate *DB 3.00098* | FortiClient *DB 3.00098* | FortiSASE *DB 3.00098* | FortiProxy *DB 3.00098*

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 *v4.0+* | FortiAnalyzer *v7.0+* | FortiSIEM *DB 6.4.0+*

IOC

Detects IOCs in historical logs across the security fabric

FortiAnalyzer *DB 0.02338* | FortiSIEM *DB 0.02338* | FortiSOCaaS *DB 0.02338*

Outbreak Detection

Detects indicators of the Exchange ProxyNotShell incident across the security fabric

FortiAnalyzer *DB 1.00064* | FortiSOCaaS *DB 1.00064*

Content Update

FortiSIEM
DB 305

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.

FortiSOAR

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

Bleeping Computer https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-day-activelty-exploited-in-attacks/

GTSC https://www.gteltsc.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/4778/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

FORTINET