Microsoft Exchange

Recently targeted by **HAFNIUM**

https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

*Firstly, if you are running an un-patched on-premise Microsoft Exchange version, you should upgrade immediately! This is a **critical** vulnerability that allows an attacker to access a desired user's mailbox, requiring only the e-mail address of the user they wish to target! These details and more were disclosed by Volexity here.*
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

The vulnerabilities affect Exchange Server 2013, 2016 and 2019. Exchange Online is not affected.

January 6, 2021 — Zero Day Exploits

In the article above, Volexity disclosed seeing these exploits as early as January 6, 2021. The first CVE discovered was CVE-2021-26855 being used to steal content from mailboxes. On further monitoring of the environments, it was observed the attacker can chain this vulnerability to others (including CVE-2021-27065), enabling remote code execution, and eventually lateral movement. More details are available from Volexity's post.

March 2, 2021 — MSFT Annoucement

On March 2, 2020, Microsoft released the patches via MSRC:
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

Volexity published their findings:
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Microsoft published further information about nation-state attacks, and identified HAFNIUM specifically as the primary threat actor exploiting these vulnerabilities:
https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Latest — Ongoing Developments

On March 3, FortiGuard released initial analysis in Threat Signal report:
https://www.fortiguard.com/threat-signal-report/3856/out-of-band-patches-for-in-the-wild-exploitation-microsoft-exchange-server

On March 5, Microsoft released additional details and mitigation techniques that can be used by customers unable to upgrade quickly:
https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

On March 11, Microsoft announced detection of a new variant of DearCry ransomware was being used on vulnerable Exchange servers: https://twitter.com/MsftSecIntel/status/1370236539427459076

Full details on Fortinet protection for DearCry is available from:
https://fndn.fortinet.net/FortiGuard-Alert-Outbreaks/Dearcry/

Fortinet Products Summary	Services	Version	Other info
FortiGate NGFW	IPS	*18.030*	Blocks the exploit (deploy NGFW in front of Exchange server)
	Anti-Virus	*84.00475*	Blocks the hashes identified by Microsoft in the blog post. Does not prevent the exploitation, but will prevent the data being exfiltrated.
FortiClient	Vulnerability	*1.234*	Detects vulnerable instance of Exchange running on Windows Server
FortiWeb	WAF	*0.00286*	Blocks the exploit (deploy WAF in front of Exchange server)
FortiEDR	EDR	*v4, v5*	Blocks post-exploitation activity including dumping the LSASS memory, running Nishang and PowerCat tool.
FortiDeceptor	Lure	*3.x*	Deception Lure for saved passwords and SMB will divert attacker to decoys and detect the attack.
	Decoy	*3.x*	Decoys in the MS Exchange segment can detect the lateral movement.
FortiAnalyzer	Event Handler Threat Hunting Report	*6.2, 6.4*	Raise event when FortiGate IPS detects a vulnerable instance exploit attempt, or AV detects a known IOC.
FortiSIEM	Rules & Threat Hunting Report	*5.x, 6.x*	Detects indicators attributed to Hafnium from IIS logs, Windows, FortiGate IPS and Virus logs, Network Traffic logs.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

This is a critical vulnerability of a supported / trusted Microsoft Exchange instance, and affects the on-premise deployments of Exchange 2013, 2016 and 2019.

Detect Vulnerable App
FortiClient Vulnerability Package Update
Version Info: 1.234
Link: https://www.fortiguard.com/updates/epvuln?version=1.234

Exploitation

*Multiple products & services including **FortiGuard IPS** and **FortiWeb** detect & prevent the exploit and lateral movements within the Enterprise network.*

Block Exploit with IPS
FortiGate IPS Database Update
Version Info: 18.030 (and 18.028)
Link: https://www.fortiguard.com/updates/ips?version=18.030

Block Exploit with FortiWeb
FortiWeb Web Security Update
Version Info: 0.00286
Link: https://www.fortiguard.com/updates/websecurity?version=0.00286

Installation

*Multiple products & services including **FortiEDR** and **FortiGuard AntiVirus** detect & defuse exploited system activities.*

Defuse Exploit
FortiEDR (with optional **MDR** and **XDR** services)
Version Info: v4, v5
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD52016
Other Info: Blocks post-exploitation activity including dumping the LSASS memory, running Nishang and PowerCat tools.

Defuse Exfiltration Attempts
FortiGate / FortiGuard Anti-Virus
Version Info: 84.00473
Link: https://www.fortiguard.com/updates/antivirus?version=84.00475
Other Info: Blocks the hashes identified by Microsoft in the blog post. Does not prevent the exploitation, but will prevent the data being exfiltrated.

Detect& Defuse Lateral Movement
FortiDeceptor Lure (saved password & cache credentials) + Deception Decoy
Version Info: 3.x
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD52018
Other Info: Deception Lure for saved passwords and SMB will divert attacker to decoys and detect the attack. Decoys in the MS Exchange segment can detect the lateral movement.

C2

Action

DearCry Ransomware
Multiple Fortinet Protections
Link: https://fndn.fortinet.net/FortiGuard-Alert-Outbreaks/Dearcry/
Other Info: One of the common attacks been launched in 2nd stage, as reported by MSFT.

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

Threat Hunting Report
FortiAnalyzer Report
Version Info: n/a
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD51568
Other Info: Detects indicators based on FortiGate IPS and AV.

Event Handler
FortiAnalyzer Event Handler
Version Info: FortiAnalyzer 6.2, 6.4
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD51568
Other Info: Detects indicators based on FortiGate IPS and AV.

SIEM Threat Hunting Report
FortiSIEM Report
Version Info: 5.x and 6.x
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD51618
Other Info: Detects indicators attributed to Hafnium from IIS logs, Windows, FortiGate IPS and Virus logs, Network Traffic logs

SIEM Rules
FortiSIEM Rules
Version Info: 5.x and 6.x
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD51618
Other Info: Detects indicators attributed to Hafnium from IIS logs, Windows, FortiGate IPS and Virus logs, Network Traffic logs