0

Ò

D

OUTBREAK ALERTS 🗘



Targeted by HAFNIUM

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ CVEs: CVE-2021-26855, CVE-2021-27065

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.

Background	In the article above, Volexity disclosed seeing these exploits as early as January 3, 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.
Announced	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/
Latest Developments	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/
	Microsoft published further information about nation-state attacks, and identified HAFNIUM specifically as the primary threat actor exploiting these vulnerabilities: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/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/
	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
	OTECT ermeasures across the security fabric for protecting assets, data and network from cybersecurity
Reconnaise Lure	sance
FortiDeceptor v3.0+	
Decoy VN	Л
E	

FortiDeceptor v3.0+ Weaponization Delivery

AV						
ocks the has Ita being exfi	shes identified by iltrated.	/ Microsoft in th	e blog post. Doe	es not prevent th	ne exploitation, I	but will prevent
		Ŀ			< <u></u>	<*>>
FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 84.00475	DB 84.00475	DB 84.00475	DB 84.00475	DB 84.00475	DB 84.00475	DB 84.00475
FortiProxy						
DB 84.00475						
A)/ (Dro fil	tor					
AV (Pre-fil						
locks the has ata being exfi	shes identified by iltrated.	/ Microsoft in th	e blog post. Do	es not prevent th	ne exploitation, I	but will prevent
FortiEDR	FortiSandbox	FortiNDR				
DB 84.00475	DB 84.00475	DB 84.00475				
xploitatior	ı					
IPS						
locks the exp	oloit (deploy NGF	W in front of Ex	change server)			
	æ					
FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy		
DB 18.03	DB 18.03	DB 18.03	DB 18.03	DB 18.03		
Web App \$	Security					
locks the exp	oloit (deploy WAF	in front of Excl	hange server)			
FortiWeb						
DB 0.00286						
DB 0.00286						

Post-execution

Blocks post-exploitation activity including dumping the LSASS memory, running Nishang and PowerCat tool

	FortiEDR
	<i>v4.0</i> +
ò	C2
Ĭ	Action
	Action
	DETEAT
	DETECT
	Find and correlate important information to identify an outbreak, the following updates are available to ra
	alert and generate reports:
.	
Y	Outbreak Detection
	FortiAnalyzer
	FortiAnalyzer
	FortiAnalyzer DB 1.00033
	DB 1.00033
	DB 1.00033
	DB 1.00033 Threat Hunting
	DB 1.00033 Threat Hunting
	DB 1.00033
	DB 1.00033 Threat Hunting
	DB 1.00033

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.



FortiXDR

Assisted Response Services

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

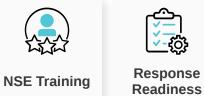




Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.



IDENTIFY Identify processes and assets that need protection:
Attack Surface Hardening
Check Security Fabric devices to build actionable configuration recommendations and key indicators.
Security Rating
Vulnerability Management
Reduce the attack surface on software vulnerabilities via systematic and automated patching.
FortiEDR

Additional Resources

Microsoft

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Volexity

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

Learn more about FortiGuard Outbreak Alerts

