

Microsoft Exchange Server RCE Vulnerabilities

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/MstfSecIntel/status/1370236539427459076>

PROTECT

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

Reconnaissance

Lure

FortiDeceptor
v3.0+

Decoy VM

FortiDeceptor
v3.0+

Weaponization

Delivery

AV

Blocks the hashes identified by Microsoft in the blog post. Does not prevent the exploitation, but will prevent the data being exfiltrated.

FortiGate
DB 84.00475

FortiWeb
DB 84.00475

FortiClient
DB 84.00475

FortiSASE
DB 84.00475

FortiMail
DB 84.00475

FortiCASB
DB 84.00475

FortiCWP
DB 84.00475

FortiProxy
DB 84.00475

AV (Pre-filter)

Blocks the hashes identified by Microsoft in the blog post. Does not prevent the exploitation, but will prevent the data being exfiltrated.

FortiEDR
DB 84.00475

FortiSandbox
DB 84.00475

FortiNDR
DB 84.00475

Exploitation

IPS

Blocks the exploit (deploy NGFW in front of Exchange server)

FortiGate
DB 18.03

FortiSASE
DB 18.03

FortiNDR
DB 18.03

FortiADC
DB 18.03

FortiProxy
DB 18.03

Web App Security

Blocks the exploit (deploy WAF in front of Exchange server)

FortiWeb
DB 0.00286

Installation

Post-execution

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

FortiEDR
v4.0+

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

FortiAnalyzer
DB 1.00033

Threat Hunting

FortiAnalyzer
v6.2+

FortiSIEM
v5.0+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

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

Incident Response

RECOVER

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.

NSE Training

Response Readiness

End-User Training

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

Security Awareness & Training

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](#)