Tools for Detection of Compromise of Microsoft Exchange Server Vulnerabilities

Executive Summary

Microsoft released patches for four Exchange Server zero-day vulnerabilities on March 2, 2021. They are being actively and aggressively exploited by sophisticated state-sponsored threat actors who have a history of targeting healthcare organizations. Since the release of the patches, several tools have been released which can aid in detecting exploitation as well as persistent access backdoors known to be used in these attacks. These tools should be considered as part of an overall defense strategy. This analyst note is a follow-up to the note we released on March 3.

Report

On March 2, 2021, Microsoft released emergency out-of-band security updates for four Microsoft Exchange zero-day vulnerabilities (collectively referred to as ProLogon) being actively exploited in targeted attacks. These flaws affect Microsoft Exchange Server versions 2013, 2016, and 2019. Exchange Online (O365) is not affected. Microsoft reported that these vulnerabilities are being attacked by a Chinese state-sponsored cyber actor who has a history of heavily targeting US organizations across industries, but most notably, infectious disease researchers. Other researchers and journalists have reported that over 30,000 US organizations have already been compromised to date, and as such, testing and implementing the patches should be done with a high priority. The Cybersecurity and Infrastructure Agency (CISA) released an emergency directive (ED-2102) Mitigate Microsoft Exchange On-Premises Product Vulnerabilities with required actions for related federal agencies specifically tailored to Microsoft Exchange on-premises products. HC3 released an analyst note (202103031700) on March 3 which describes this in further detail.

Recommended Actions

Microsoft has since released a number of tools to assist in detection and mitigation of this threat. These include a PowerShell script on GitHub with a list of commands that an Exchange administrator to use to detect if they were compromised. This script automates the four commands found in the Hafnium blog post. It includes a progress bar and performance enhancements to speed up the CVE-2021-26855 test.

Microsoft also updated signatures for Defender that will detect the web shells installed using the zero-day vulnerabilities (these web shells are for persistence, so even if a system has been patched, the web shells will allow the attackers to maintain access and launch follow-up cyberattacks). For organizations that don't use Defender, Microsoft has added the updated signatures to their Microsoft Safety Scanner standalone tool to assist organizations in identifying and removing these web shells. It's also known as the Microsoft Support Emergency Response Tool (MSERT) and is a portable antimalware tool which includes Microsoft Defender signatures to scan for and remove detected malware.

The national Computer Emergency Response Team (CERT) for the country of Latvia has also released a tool on Github to detect the presence of the web shell being deployed as part of the MS Exchange compromise. It's also a PowerShell script and instructions are included on the page.

HC3 products can be found on our website: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

References

Microsoft fixes actively exploited Exchange zero-day bugs, patch now
https://www.bleepingcomputer.com/news/security/microsoft-fixes-actively-exploited-exchange-zero-day-bugs-patch-now/

HAFNIUM targeting Exchange Servers with 0-day exploits
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Microsoft Patches Four Zero-Day Exchange Server Bugs
https://www.infosecurity-magazine.com/news/microsoft-patch-four-zeroday/

Microsoft: Multiple Security Updates Released for Exchange Server
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

Microsoft Fixes Exchange Server Zero-Days Exploited in Active Attacks
https://www.darkreading.com/threat-intelligence/microsoft-fixes-exchange-server-zero-days-exploited-in-active-attacks/d/d-id/1340305

Exchange Servers targeted via zero-day exploits, have yours been hit?
https://www.helpnetsecurity.com/2021/03/03/exchange-servers-zero-day/

State hackers rush to exploit unpatched Microsoft Exchange servers
https://www.bleepingcomputer.com/news/security/state-hackers-rush-to-exploit-unpatched-microsoft-exchange-servers/

CISA Emergency Directive 21-02
https://cyber.dhs.gov/ed/21-02/

Latvia CERT Homepage
https://www.cert.lv/en

A Basic Timeline of the Exchange Mass-Hack
https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

Update to Alert on Mitigating Microsoft Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/03/04/update-alert-mitigating-microsoft-exchange-server-vulnerabilities

HC3 products
https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software
https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

CSS-Exchange on Microsoft GitHub Repository
https://github.com/microsoft/CSS-Exchange/tree/main/Security

Microsoft Safety Scanner
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Latvia Cert Exchange Webshell Detector
https://github.com/cert-lv/exchange_webshell_detection

Chinese Hacking Spree Hit an 'Astronomical' Number of Victims
https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/

This new Microsoft tool checks Exchange Servers for ProxyLogon hacks
https://www.bleepingcomputer.com/news/microsoft/this-new-microsoft-tool-checks-exchange-servers-for-proxylogon-hacks/

China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers
https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991

Move over, SolarWinds: 30,000 orgs' email hacked via Microsoft Exchange Server flaws
https://www.theverge.com/2021/3/5/22316189/microsoft-exchange-server-security-exploit-china-attack-30000-organizations

CISA: Microsoft IOC Detection Tool for Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/03/06/microsoft-ioc-detection-tool-exchange-server-vulnerabilities

CISA: Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/03/05/microsoft-releases-alternative-mitigations-exchange-server

Microsoft Attack Blamed on China Morphs Into Global Crisis
https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world

Microsoft's MSERT tool now finds web shells from Exchange Server attacks
https://www.bleepingcomputer.com/news/security/microsofts-msert-tool-now-finds-web-shells-from-exchange-server-attacks/