Microsoft Patches Zero-Day Vulnerabilities Being Actively Exploited by a Threat Actor who has Historically Targeted Healthcare Organizations

Executive Summary

Microsoft released patches for four Exchange Server zero-day vulnerabilities that are being actively exploited by sophisticated threat actors who have a history of targeting healthcare organizations with cyberattacks.

Report

On March 2, 2021, Microsoft released emergency out-of-band security updates for four Microsoft Exchange zero-day vulnerabilities being actively exploited in targeted attacks. These flaws affect Microsoft Exchange Server versions 2013, 2016, and 2019. Exchange Online (O365) is not affected. Microsoft has labeled the group that is actively attacking vulnerable Exchange servers HAFNIUM who, according to them is Chinese state-sponsored and has a history of heavily targeting US organizations across industries, but most notably, infectious disease researchers. Other researchers have identified other threat actors, believed to be China-based, to be exploiting these vulnerabilities as well.

The initial attack requires the ability to make an untrusted connection to Exchange server port 443. Following that, the listed zero-day vulnerabilities are being exploited:

CVE-2021-26855 – A server-side request forgery vulnerability which allows an attacker to send arbitrary HTTP requests and authenticate to the exchange server.

CVE-2021-26857 – A remote code execution vulnerability via insecure deserialization which means untrusted user-controllable data is deserialized (structure is changed for storage or transmission) by an application/process.

CVE-2021-26858 – A remote code execution vulnerability, more specifically a post authentication arbitrary file-write vulnerability, that requires either the exploitation of the first vulnerability (26855) or compromising legitimate administrative credentials first.

CVE-2021-27065 – Similar to 26858, this is another remote code execution vulnerability, in the form of a post authentication arbitrary file-write vulnerability, which also requires either the exploitation of the first vulnerability (26855) or compromising legitimate administrative credentials first.

Recommended Actions

Microsoft released patches for these vulnerabilities on March 2. The HC3 recommends that healthcare organizations identify Exchange servers in their infrastructure and patch them immediately. It's also recommended that external-facing Exchange servers receive the highest priority. Testing the patches prior to patching may also be necessary, depending on organizational risk management profile, however it is important that the patching process be expedited. As previously noted, these flaws affect Microsoft Exchange Server versions 2013, 2016, and 2019. Exchange Online (O365) is not affected. 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.

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/

CVE-2021-26858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26858

CVE-2021-26857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-26857

CVE-2021-26855
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26855

CVE-2021-27065
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27065

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