21CFS Response to combat *HAFNIUM attacks and security flaws* within Exchange Server

Closing Off the Vulnerabilities

In early 2021 a new ransomware variant gained notoriety specifically for targeting On-Premise hosted internet facing Microsoft Exchange servers. This variant was discovered to primarily target United States based businesses across many sectors of the economy including financial and banking systems providers. The danger, just as was seen in previous ransomware outbreaks, concerned encryption of files and the exfil of confidential data.

Subsequently the FDIC proactively reached out to **21CFS** and may have reached out to many of you as well to review and discuss Microsoft Exchange configurations and how they may or may not be affected. In our review with FDIC, we explained that for all corporate email traffic including all traffic between us and external sources is handled by a hosted solution hosted by Microsoft. Though we have an on-premises Microsoft Exchange server as well, it is not allowed external access as it only transmits data within our network and dedicated circuits for the purpose of system alerts and notifications, therefore exposure is limited. Furthermore, with our strict security protocols all required patches and updates are strenuously applied.

The discussion was a fruitful one and once again highlighted the cooperative nature of a good relationship with FDIC. We would highly suggest that now would be a good time to have your IT and Cybersecurity departments to immediately review and confirm all email configurations, designs, and patch levels to adequately protect against this and expected future attacks.

21CFS
INNOVATIVE BANKING

What Should Your Bank Do?

The Cybersecurity and Infrastructure Security Agency issued guidance, outlining five steps that enterprises need to take if they have Microsoft Exchange servers.

1. Create a forensic image of your system
2. Check for indicators of compromise. Microsoft has shared a tool on GitHub to help companies do just that
3. Install the latest patches from Microsoft
4. If you can't patch, follow Microsoft's mitigation instructions until you can
5. If you discover you've been compromised, implement your incident response plan. CISA has some guidance there, as well

REMEDIATING MICROSOFT EXCHANGE VULNERABILITIES

An adversary can exploit this vulnerability to compromise your network and steal information, encrypt data for ransom, or even execute a destructive attack. Leaders at all organizations must immediately address this incident by asking their IT personnel:

- What steps your organization has taken
- Whether your organization has the technical capability to follow the guidance provided below; and
- If your organization does not have the capability to follow the guidance below, whether third-party IT security support has been requested

Leaders should request frequent updates from in-house or third-party IT personnel on progress in implementing the guidance below until completed.

For IT Security Staff:

As exploitation of these vulnerabilities is widespread and indiscriminate, CISA strongly advises all system owners complete the following steps:

1. If you have the capability, follow the guidance in CISA Alert AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities to create a forensic image of your system.
2. Check for indicators of compromise (IOCs) by running the Microsoft IOC Detection Tool for Exchange Server Vulnerabilities.
3. Immediately update all instances of on-premises Microsoft Exchange that you are hosting.
4. If you are unable to immediately apply updates, follow Microsoft's alternative mitigations in the interim.

   Note: these mitigations are not an adequate long-term replacement for applying updates; organizations should apply updates as soon as possible.
5. If you have been compromised, follow the guidance in CISA Alert AA21-062A. For additional incident response guidance, see CISA Alert AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity.

   Note: Responding to IOCs is essential to evict an adversary from your network and therefore needs to occur in conjunction with measures to secure the Microsoft Exchange environment.

Additional Resources for You and Your Team to Review:

- Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
- CISA Alert AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities
- Microsoft IOC Detection Tool for Exchange Server Vulnerabilities
- *(Added March 15, 2021)* Microsoft EOMT.ps1 tool (can automate portions of both the detection and patching process)
- *(Added March 12, 2021)* Check my OWA tool for checking if a system has been affected.

***Disclaimer**: This tool does not check against an exhaustive list of compromised domains. It is meant for informational purposes only. The United States Government does not provide any warranties of any kind regarding this information and cannot assure its accuracy or completeness; therefore, entities should not rely solely on this information to justify foregoing CISA's recommendations for action described in this newsletter.*

- *(Released March 10, 2021)* Joint FBI-CISA Cybersecurity Advisory AA21-069A: Compromise of Microsoft Exchange Server
- *(Updated)* Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability
- CISA Alert AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity
- *(Updated)* Microsoft Advisory: Multiple Security Updates Released for Exchange Server
- Microsoft Security Blog: Hafnium targeting Exchange Servers
- Volexity Blog: Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities
- Microsoft Security Response Center Blog: Microsoft Exchange Server Vulnerabilities Mitigations
- CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide

If you should have any questions, 21 CFS is here to help.

Contact us at:

Direct: 512-490-2505

Toll free: 866-398-2178

21st Century Financial Services
10711 Burnet Rd., Ste. 306
Austin, TX 78758