IT Security   Supply Chain   OT Security   Insider Threat   Physical Security   Interoperable Communications

MITIGATE MICROSOFT EXCHANGE ON-PREMISES PRODUCT VULNERABILITIES

CISA PARTNERS:

The Cybersecurity and Infrastructure Security Agency (CISA) strongly urges its partners to follow guidance provided to Federal Civilian Executive Branch Departments and Agencies at cisa.gov/ED2102. This CISA Emergency Directive outlines key steps federal officials must take to immediately address this vulnerability.

The seriousness of this vulnerability cannot be overstated; the exploitation of it is widespread and is indiscriminate.

CISA published a **Current Activity** supplemental guidance March 5, to ensure all partners understand the severity of the vulnerability and steps to detect and mitigate potential compromise. All information surrounding this vulnerability can also be found directly at **cisa.gov/ED2102**.

NOTE: Exploitation of this vulnerability, while you are vulnerable, permits an adversary to compromise identity and trust in your network, which is likely to persist even after patching Exchange. Please immediately speak with your IT officials to determine what steps your organization has taken, and if your organization does not have the technical capability to verify network integrity, please consider bringing in a third party to assist you as soon as possible.

Everyone using Microsoft Exchange on-premise products needs to immediately:

- Check for signs of compromise;
- If evidence of compromise is found, assume that your organization's network identity has been compromised and begin incident response procedures
- Patch Microsoft Exchange with the vendor released patches;
- If unable to patch immediately or remove the Microsoft Exchange from the network immediately, CISA strongly recommends following alternative mitigations found in Microsoft's blog on Exchange Server Vulnerabilities Mitigations. This should not be taken as an adequate solution for patching.

Response to indicators of compromise are essential to eradicate adversaries already on your network and must be accomplished in conjunction with measures to secure the Microsoft Exchange environment.

Patching an already compromised system will not be sufficient to mitigate this situation; therefore, CISA strongly encourages partners to immediately disconnect any Microsoft Exchange systems suspected of being compromised.

Please contact CISA for any questions or to report an incident regarding this vulnerability at **Central@cisa.gov**.

ACTIONS FOR IT ADMINS/STAFF

CISA is tracking a serious issue with Microsoft Exchange. CISA cannot emphasize enough that exploitation is widespread and indiscriminate, and we are advising all system owners to complete the following actions. Please follow this checklist and provide feedback to your leadership on the actions you have taken and any challenges completing the steps below.

□ Patch ALL instances of Microsoft Exchange that you are hosting.

□ If you can't patch then follow the recommendations Microsoft issued – **Microsoft Exchange Server Vulnerabilities Mitigations – March 2021 – Microsoft Security Response Center** .

□ Check for indicators of compromise by running the following **script** .

□ If you have been compromised, follow this **guidance** to better understand what to do next.