Cyber Alert

On March 2nd, 2021, CISA, NSA, Microsoft, and Volexity disclosed four previously unknown vulnerabilities in Microsoft Exchange on-premises products which permit an attacker to gain persistent access to and control of an enterprise network.

Please see the below notes form the CISA call ealier today.

CISA Talking Points
Mitigation of Microsoft Exchange On-Premises Vulnerabilities
Last Updated: 11:33am EST Thursday 4 MAR 2021

- On March 2nd, 2021, CISA, NSA, Microsoft, and Volexity disclosed four previously unknown vulnerabilities in Microsoft Exchange on-premises products which permit an attacker to gain persistent access to and control of an enterprise network.
    - Microsoft has released a patch for the vulnerabilities [DETAILS]
    - The vulnerability is not currently known to affect Microsoft Azure or Office 365 cloud services
- **CISA recommends that the vulnerabilities be patched IMMEDIATELY on all networks operating any form of on-premises Microsoft Exchange** and where possible, examine their networks for known indicators of compromise [See AA]
    - Federal Civilian Agency network operators are required by CISA's March 3rd Emergency Directive 21-02 to take immediate action as described within [21-02]
    - The public is encouraged to follow similar procedures, but in any event to patch as soon as possible if rapid forensic analysis is not feasible
- Volexity and Microsoft have observed China-based malicious actors using these vulnerabilities to gain access to specifically targeted organizations within the United States.
    - Once adversaries gain access to a Microsoft Exchange on-premise server, they can likely issue credentials which would allow them to access and control an enterprise network even after the vulnerability is patched
    - Adversaries can likely use the unauthorized access to compromise other systems within an enterprise network
- Scripts automating the exploitation of this vulnerability are already available to the public and have been observed in use.
- CISA is aware of widespread exploitation of the vulnerability, which now requires less skill to execute: **operators of vulnerable systems should patch immediately**
    - Malicious exploitation can be conducted by people with any intent, to include, or physical damage to connected infrastructure
- CISA continues to assist infrastructure operators and federal agencies seeking to protect their networks, with help from our interagency and industry partners, and will release updated information as it becomes available.

This is an open-source product. Redistribution is encouraged.

View Virginia Fusion Center Homepage
Click Here

Observe Suspicious Activity?
Report Online

Not a VFC Shield Member?

Join Today!

Awareness through information sharing

This bulletin is the result of collaboration and cooperation from a variety of SHIELD programs and public safety orientated officials. Special thanks to the following partners.

VFC Shield

"Awareness Through Information Sharing"

NEED HELP WITH THIS EMAIL?

View in a browser

Download as a PDF

USEFUL LINKS

- VFC Fusion Site
- Shield Homepage
- All Products
- Report SAR
- Email Coordinator