Community Advisory: New Microsoft Exchange Server Vulnerability

A new remote code execution vulnerability (CVE-2021-42321) has been discovered which affects on-premises Microsoft Exchange Servers 2013, 2016 and 2019 and servers in Exchange Hybrid Mode. This is a Remote Code Execution (RCE) vulnerability which can allow an attacker to execute commands remotely on a targeted system to gain privileged access, deploy malware, move laterally to additional systems, and more. This is ranked as a high-severity vulnerability and hackers are targeting unpatched Exchange servers in the wild.

What You Need to Do

A patch is available from Microsoft. LMG urges all organizations to *immediately* patch, then check and determine whether your organization has been impacted by this vulnerability.

- **Patch your server immediately:** https://aka.ms/ExchangeUpdateWizard.
- **Identify servers that need to be updated**. You can use the latest version of the Exchange Server Health Checker script to verify patch status.
- **Perform an immediate search of all on-premises or hybrid Exchange servers for indicators of unauthorized access** or data exfiltration.
- **To check if your server was compromised,** follow the instructions in the "FAQ" section of the following Microsoft article: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2021-exchange-server-security-updates/ba-p/2933169.
- **If indicators of compromise are found:**
    - **Initiate your incident response procedures.** Make sure to acquire a full disk image of the server, or if that is not possible, capture (at least) volatile memory, event logs, system web logs, the registry, and filesystem metadata in addition to any available network or firewall logs.
    - **Immediately conduct proactive threat hunting** on your network to identify and remove any threats.
- **Configure your endpoint detection and IDS/IPS systems** to detect suspicious activity.
- **Ensure that your backups are working properly and can't be overwritten** in case ransomware hits. Make sure to backup server configuration files in addition to data repositories.

For more information and **to see the Exchange vulnerability in action, register for our 12/8 webinar:** https://www.lmgsecurity.com/event/cyber-alert-new-microsoft-exchange-vulnerabilities/.

Stay Up-to-Date

LMG will continue to monitor the developing situation and provide updates as they become available. If you have any questions or suspect that your network may have been compromised, please email info@LMGsecurity.com immediately for assistance.

Email: info@LMGsecurity.com; Hotline: 406-830-3165 x 1