Risk Control

RISK ALERT: Vulnerability in Microsoft Exchange Exposes Organizations to Cybersecurity Risk

On March 2, 2021, Microsoft released emergency updates to patch security vulnerabilities in Microsoft Exchange Server (MS Exchange) versions 2010, 2013, 2016 and 2019. Since then, it has been discovered that a foreign espionage group exploited vulnerabilities in MS Exchange and infiltrated at least 30,000 organizations in the United States, including a significant number of small to mid-sized businesses and local governments. An infiltration could allow unauthorized access to email environments hosted on the aforementioned MS Exchange servers, allowing intruders to install additional malware to facilitate long-term exploitation. Other consequences of a successful intrusion may include corruption of a business's network, theft of sensitive information, or data being held for ransom.

The cybersecurity community has been vigorously monitoring the active exploitation of vulnerabilities in MS Exchange servers because the attacks have continued even after Microsoft disclosed the exploit and deployed patches. Below are suggested steps to help determine whether your organization may have been a victim of the attack and to help address the underlying vulnerabilities.

The mitigation measures suggested below may appear dauntingly technical to some. As such, it is recommended that organizations consider enlisting the services of a qualified IT professional to implement them. While the following is not a comprehensive list of potential risk mitigation measures, they are options to be considered and adapted to suit the specific needs of your organization.

Exploited Vulnerability Mitigation Measures

1. Determine whether your firm utilizes one of the on-premise versions of MS Exchange identified above, and scan the suspected server for existing vulnerabilities. See Microsoft's guidelines for identification.
2. The Common Vulnerabilities and Exposures (CVE) IDs for the specific vulnerabilities determined to have been exploited are the following:
   - CVE-2021-26855
   - CVE-2021-26857
   - CVE-2021-26858
   - CVE-2021-27065

   Engage the assistance of a qualified IT professional to apply mitigation strategies suggested by Microsoft to address the vulnerabilities listed above:

   Notably, if your organization's MS Exchange server already was affected before the emergency patch was installed, you remain at risk and additional remediation measures will be required.
3. Review your organization's MS Exchange environment for Indicators of Compromise (IoC) following Microsoft's guidance to determine whether any exist. Conduct an investigation to implement proactive preventions of future exploitations.

Additional Mitigation Measures

In addition to the specific measures outlined above to address these exploited vulnerabilities, it is recommended that the following general measures be implemented to reduce the organization's exposure:

- Block known bad IP addresses at the firewall, as well as any IP addresses where a large amount of data is being sent.
- Consider resetting user credentials for the systems and IT resources used by the organization.
- Run a full anti-virus scan against the entire computing environment and not just the vulnerable servers.
- Consult additional mitigation and remediation guidelines issued by the Cybersecurity & Infrastructure Security Agency.

Closing Thoughts

This most recent attack once again highlights basic but critical steps that should be part of any organization's cybersecurity program:

- Apply security patches within 30 days of release. Organizations should check regularly for vendor-issued patches for all systems used. Often, organizations perform routine patch checks for their operating systems but not for other applications such as web browsers and mobile devices.
- Adopt and enforce strict password and credential policies. Passwords should be complex, unique and of sufficient length to defend against brute force attacks. Consider recommending that employees use a password management tool.
- Adopt quarterly phishing campaigns as part of a continuing security awareness education program. Human behavior in social engineering attacks remains a weak link in cybersecurity management.
- Conduct full system vulnerability scans on a regular basis and remediate vulnerabilities identified.

CNA CyberPrep

CNA CyberPrep, built on nearly two decades of cyber insurance expertise, is a proactive program of value-added cyber risk services developed by CNA Risk Control and CNA Cyber insurance underwriters along with leading cybersecurity specialists. It is designed to aid CNA Cyber policyholders in cyber threat identification, mitigation and response. It is available to all CNA Cyber policyholders.

Learn more about CNA CyberPrep.