RANSOMWARE TASK FORCE

Emergency Cybersecurity and Ransomware Notice

Potential for imminent financial loss and operational disruption for some Microsoft customers

March 12, 2021
Ransomware Task Force

Situation: Some organizations that use on-premises Microsoft Exchange Server for email management are at **imminent risk of financial loss, data breach, and business disruption.** Cybercriminals are already launching attacks whose severity and scale will increase over the weekend. Absent immediate action, your business could suffer serious damage.

Action: Engage your IT team immediately to take steps outlined by the U.S. Cybersecurity and Infrastructure Security Agency and Microsoft alerts to (a) patch the underlying security flaw; (b) identify any security breaches; and (c) evict any cybercriminals from your network.

What is the problem?

- A dangerous vulnerability in on-premises Microsoft Exchange Server email management systems could presently expose your organization to **imminent business interruption, financial loss and unknown legal liability**.

- On March 2, Microsoft released a software update to close critical security vulnerabilities in all versions of its most popular on-premises business email service called Microsoft Exchange Server (an on-premises email service).

- The U.S. government has confirmed that cybercriminals are actively attacking Microsoft customers who have not installed Microsoft's March 2021 software update. These attacks are increasing in severity and scale, as criminals race to harm businesses and individuals throughout the world.

- If your business has not applied the latest updates for Microsoft Exchange Server (an on-premises email service), any computer criminal could potentially compromise your computer systems *at any time*, steal and delete emails, attachments, and other proprietary information, gain total control of your IT system, and harm your business operations.

- It is critical that you **patch this vulnerability immediately by applying the update.** In addition to patching, it is equally important that you investigate all related systems and remediate any security breach you have already experienced. The U.S. government and the cybersecurity industry are classifying this as an emergency facing every business sector.

What should I do?

Step 1: Find out if you are vulnerable. Identify if your business uses any instances of on-premises **Microsoft Exchange Server**, a software product that makes it easier for businesses to manage their own email service.

- Ask whomever manages your IT systems: “Is our business using an instance of on-premises Microsoft Exchange Server?”
    - **If the answer is YES, proceed to Step 2.**
    - **If the answer is NO, disregard this document**.

Step 2: Close the vulnerability immediately.

- Ask your IT manager: “Have you downloaded the latest Microsoft software update that closes the security vulnerability in Microsoft Exchange Server?”
    - **If the answer is YES, go to Step 3.**
    - **If the answer is NO, direct them to Microsoft’s instructions immediately: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901**

Step 3: Check for a security breach. Investigate whether bad actors already entered your network before you installed the Microsoft security update.

- Instruct your IT manager to review your business IT systems for evidence that computer criminals gained access. Ensure your IT teams consider:
    - Scanning systems for evidence of bad actors by running the Microsoft Safety Scanner.
    - These technical instructions for hunting bad actors in your network.
- If your IT manager is unable to investigate potential compromise inside your business, ask your legal counsel, insurance company, or local Chamber of Commerce for assistance in hiring outside IT experts.

CONTACT: If your organization uses on-premises Microsoft Exchange Server and you are unsure how to act, determine whether your organization has the technical capability to address the vulnerabilities or consider requesting third-party IT security support. See the U.S. Cybersecurity and Infrastructure Security Agency web page for additional guidance and contact information: Remediating Microsoft Exchange Vulnerabilities.

You can find more information on the Ransomware Task Force at this website: https://securityandtechnology.org/ransomwaretaskforce/.
