LOCKTON
UNCOMMONLY INDEPENDENT

Alert

Attacks exploiting Microsoft Exchange Server flaws: What you need to know

The threat

On March 2, 2021 Microsoft reported that it has observed targeted attacks that take advantage of four zero-day vulnerabilities in Microsoft Exchange Server to gain full access to all email on the victim's system. The attacks do not affect Exchange Online. Technical information about the attacks is available in this report by the cybersecurity firm FireEye.

The attacks began in January 2021 and grew in February. Tens of thousands of servers reportedly have been affected. The attacks are continuing.

A hacker group in China known as "Hafnium" is believed to be responsible for the attacks. "Hafnium" reportedly is sponsored by the Chinese government.

Microsoft has released security updates for the affected Exchange products (Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019). The company recommends that they be applied immediately.

The seriousness of the attack led the U.S. government to issue an emergency directive on March 3, 2021 requiring all federal agencies to immediately apply the Microsoft security updates if there are no indications of compromise.

What you should do

Organizations using the affected Microsoft Exchange Server products should immediately determine whether they are vulnerable to attack. Microsoft has created a script that can do that. The script can be downloaded from this page.

Lockton strongly recommends that potentially affected organizations run the Microsoft test immediately.

If the Exchange Server vulnerabilities exist on your organization's system, it is essential to then determine if an attack is in progress. This article by Splunk, a cybersecurity and IT operations firm, provides helpful guidance for organizations navigating that process.

It is essential that the Microsoft security updates be applied as soon as possible.

Organizations also need to be concerned about their supply chain vendors. They should ask their vendors the following questions:

- Does the Organization have a master vendor list of who they share information with? Does the vendor utilize any of the affected Exchange products? ○ If yes, has the vendor applied the recommended Microsoft security updates?
    - If no, when will the vendor apply the security updates?
- Does the vendor utilize any vendors that rely on the affected Exchange products?

If yes, what has the vendor done to mitigate this potential risk?

Cyber insurance concerns

A Hafnium attack should trigger any cyber insurance an organization has in place. The costs to respond to the attack and to comply with any notification or other legal obligations flowing from the event should be covered. A good policy should also cover any cost incurred to restore or recreate any data that is damaged, and any loss resulting from any interruption in the organization's business caused by the attack. A cyber policy should also cover any legal liability the organization has to regulators and/or individuals whose private information may have been compromised.

Cyber policies typically give insureds the option to notify the insurer of circumstances that may lead to loss covered by the policy. While it may be tempting for organizations running affected Exchange Server products to notify their cyber insurers, Lockton recommends doing so only if the organization discovers that the vulnerabilities being exploited are present in the system. If the organization discovers that an attack is underway, it should be reported to cyber insurers immediately.

Looking ahead, we expect cyber insurance underwriters to begin asking questions about the existence of vulnerabilities that make the Hafnium attacks possible. We believe it is likely that insurers will decline to insure organizations that have not remediated those vulnerabilities.

The Hafnium attacks are a good reminder that organizations need to alertly manage their cyber risks. Lockton's Cyber Risk Control Services are here to help. If you would like to learn more about how Lockton can assist, please contact your account executive.

Peter Erceg
Senior Vice President, Global Professional & Financial Risks
T: +44 207 933 2608
E: peter.erceg@uk.lockton.com

Vanessa Cathie
Vice President, Global Professional & Financial Risks
T: +44 020 7933 2478
E: vanessa.cathie@uk.lockton.com

LOCKTON
UNCOMMONLY INDEPENDENT