Microsoft Exchange Hack - Essential Steps to Protect Your Data

On March 2, Microsoft warned of exploits that take advantage of multiple Microsoft Exchange vulnerabilities. Security experts warn that any organization running on-premises Microsoft Exchange could be at risk for the Microsoft Exchange Hack. They must take the threat seriously and follow the steps necessary to protect data assets.

Hafnium Hack

The Microsoft hack appears to have originated with the Hafnium organization out of China. Hence, some refer to it as the Hafnium Hack.

However, experts have now identified at least ten advanced persistent threat groups using the vulnerabilities to attack thousands of servers an hour. And it appears the attacks began more than two months before last week's Microsoft announcement.

Through these attacks, cyber criminals gain access to on-premises Exchange servers. Once in the system, they potentially control email accounts and install additional malware for long-term access.

The Microsoft Exchange hack or Hafnium hack potentially affects thousands of organizations worldwide. In fact, cyber security companies have begun compiling a victim list of thousands of U.S. companies, from banks to non-profits and public utilities.

In each case, hackers exploit one of four Exchange vulnerabilities. In addition to stealing data from email accounts, the criminals leave behind a hacking tool known as a web shell. Using the web shell, they can then move laterally throughout the network, stealing data and launching additional attacks.

Apply Security Patches ASAP

Last week, Microsoft released security patches for the four Exchange vulnerabilities. These apply to all on-premises Microsoft Exchange Servers. Microsoft 365 appears unaffected. Organizations should immediately identify all instances of on-premises Exchange and apply those security patches without delay. Give priority to servers accessible from the internet.

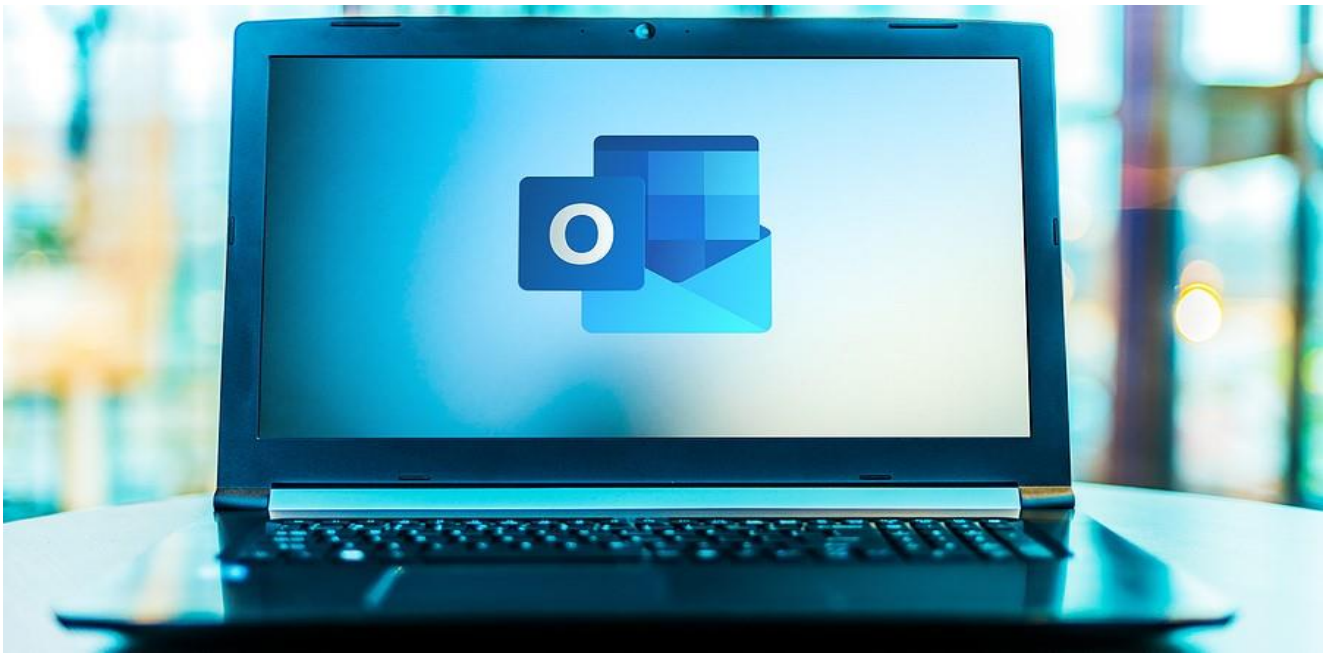
If organizations cannot update the Exchange servers immediately, they should disable external access to Exchange until they can apply the patches. Microsoft has published some interim mitigations to apply in these cases, but they stress that they do not provide long-term protection.

Keep in mind that the security patches, while critical, will not prevent damage from backdoors already installed in affected systems. In addition to installing security patches, companies must also assess their systems to check for possible compromise.

Look for Indications of System Compromise

Even if your organization applied the security patches as soon as Microsoft released them, hackers may have already gained access to your network. In addition to system updates, conduct analysis to look for anomalies that might indicate a compromised system.

To help in the forensic process, Microsoft has released a detection tool to help locate indicators of compromise (IOC). These IOCs include known malicious paths and web shell hashes that can indicate backdoors. Additional anomalies such as unauthorized account access or evidence of suspicious movement within the system also warrant further action.



If You Find Anomalies

If your system analysis uncovers evidence of possible compromise, address the situation right away. Begin with a thorough analysis of memory, windows event logs, registry hives and web logs.

Even if the hackers have not already caused damage to your data, they will be able to access your system for as long as a backdoor exists. Consequently, you must take steps to remove all traces of unauthorized presence. The longer the backdoors exist, the more damage the hackers can do.

Use Experts to Address Microsoft Exchange Hack

Identifying and addressing system compromise quickly is crucial to protecting your data. At the same time, the Microsoft Exchange hack has evolved rapidly, with new threat actors entering the scene daily. To ensure protection and avoid problems down the road, consider partnering with a third-party security expert.

The trained, certified cyber security experts at eMazzanti Technologies deliver the peace of mind you need. With deep knowledge of Microsoft and an eye on the developing security landscape, they will help you quickly safeguard your system to protect valuable data assets.