protiviti®
Face the Future with Confidence

Microsoft Discovers Multiple Zero-Day Exploits Being Used to Attack Exchange Servers

On-Premises Exchange Servers and All Hybrid Systems Impacted

March 4, 2021

On Tuesday, March 2, 2021, Microsoft released four out-of-cycle security updates for on-premises Microsoft Exchange Servers to address vulnerabilities that have been exploited in limited and targeted attacks by a previously unknown Chinese espionage group. Upon validating the attacks, Microsoft immediately shared patches of all affected systems with customers and the security community. The Microsoft Threat Intelligence Center (MSTIC) attributed the attacks to Hafnium and explained that the attackers are seeking to gain access to organizations' on-premises Exchange servers to access email accounts, exfiltrate data and install malware to maintain this access.

The U.S. Cybersecurity and Infrastructure Security (CISA) partners observed active exploitation of these vulnerabilities and, following the release of the updates, issued Emergency Directive 21-02 to federal agencies to implement a patch immediately or disconnect Microsoft Exchange servers from the Internet. Given the nature of the threat and its potential impact to a number of industry sectors, organizations should take proactive steps to apply these security updates immediately to affected systems and also should evaluate their incident response function to ensure an appropriate level of vigilance.

Systems Affected

All on-premises Exchange servers and hybrid Exchange systems are affected.

Important to note: It is extremely likely that any system with an on-premises Active Directory (AD) uses an on-premises Exchange server for connectivity.

Steps to Take

- **Scan** – Obtain an inventory of the patch-level status of all on-premises Exchange servers. Protiviti has assessed the YARA rules and verified that they accurately address the indicators known on March 2, 2021.

- **Patch** – Apply the security updates to Exchange Server 2010, 2013, 2016 and 2019. Exchange Online is not affected. Microsoft has published a blog post that discusses the security updates in more detail and answers questions around the installation of these patches. The vulnerabilities being exploited are CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065. Organizations should read the patch release notes carefully and understand the requirements before installing the security updates. Microsoft has provided a rollup patch for these vulnerabilities that may require the installation of previous rollups. Additionally, the SANS Institute is regularly updating a summary of patches and vulnerabilities known to be exploited.

- **Detect** – Assess whether on-premises Exchange and other systems have been impacted. Microsoft has provided indicators of compromise (IOCs), detection guidance and advanced hunting queries to help organizations search for signs of compromise and prevent future attacks. Microsoft Defender has released updated signatures to detect known attacks used against this vulnerability.

- **Review Identity and Access Management Program and Systems** – The strength of an organization's identity and access management (IAM) program and systems is critical to an attacker's ability to gain and maintain unauthorized access to the organization's environment. Elements like privileged access management (PAM), identity federation, session management, service account management and other core disciplines within an IAM program all play a crucial role in defending the organization. This is a good time for organizations to evaluate their IAM program and ensure adequate defense-in-depth against this and similar attack vectors.

How Protiviti Can Help

Protiviti can assist companies with preparing for and responding to the evolving threats posed by zero-day vulnerabilities with services such as our Microsoft 365 Incident Response. Contact Protiviti's Incident Response Team at IR@protiviti.com for technical, crisis management and investigative support.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.