SENT 11-11-2021.
ATTACHMENTS: 0

View this email in your browser

SANDBOX TECHNOLOGIES

Microsoft Exchange Exploit Notification

Microsoft has discovered a new exploit affecting users of Microsoft Exchange Server. The exploit, CVE-2021-42321 can allow an attacker to gain "super user" level access to Exchange upon successfully breaching any authorized user of the system.

According to Microsoft "*The November 2021 security updates for Exchange Server address vulnerabilities reported by security partners and found through Microsoft's internal processes. We are aware of limited targeted attacks in the wild using one of vulnerabilities (CVE-2021-42321), which is a post-authentication vulnerability in Exchange 2016 and 2019. Our recommendation is to install these updates immediately to protect your environment*."

Although the attacker must be authenticated to exploit this vulnerability, the confidentiality and integrity scores are listed as high, which means successful execution gives the attacker access to Exchange at a super user level if any authorized user is breached, and thus Microsoft is recommending that these be patched right away.

If you have received this notification, our records indicate that your organization employs the use of the unsupported 2010 version of Microsoft's Exchange Server software. Because Microsoft has discontinued support for this version, no patch has been made available to address the above exploit.

Although Microsoft does not specifically state whether or not the aforementioned exploit affects unsupported versions of Exchange, from the fact that it impacts users of Exchange 2013, 2016 and 2019 leads us to infer that older software versions may also be vulnerable.

For this reason, we are recommending extra vigilance, and retirement of your existing software as soon as possible by either upgrading to a supported version, or migrating to the cloud-hosted Microsoft365 platform. If you have questions or would like additional information about potential risks and/or upgrade options, please contact your Consulting CIO, or reply to this message and request that you be contacted.

Aaron Arlotti
Manager, Remote Support Operations
Sandbox Technologies, Inc.

Our mailing address is:

4111 West Alameda Ave., Suite 605 Burbank, CA 91505