Microsoft Exchange Server 2013 Reaches End of Support

Microsoft Exchange Server 2013 has reached end of support on April 11, 2023, and will no longer receive security patches.

The product will continue to work even after this date, but Microsoft is no longer providing technical support, bug fixes for usability and stability issues, time zone updates, and, importantly, fixes for vulnerabilities that could expose servers to hacker attacks.

Microsoft reminded users in February about Exchange Server 2013 approaching end of support, advising them to migrate to Exchange 2019 or Exchange Online (Microsoft 365 or Office 365).

The tech giant has provided detailed instructions for users who have yet to migrate. The company has made no mention about extended support being available.

It’s important that organizations stop using Exchange 2013 considering that the product has often been targeted in attacks, including by profit-driven cybercriminals and state-sponsored threat actors.

“Attackers looking to exploit unpatched Exchange servers are not going to go away,” Microsoft warned in January.

The US Cybersecurity and Infrastructure Security Agency (CISA) is currently aware of 16 Microsoft Exchange vulnerabilities that have been exploited in the wild. The list includes the flaws tracked as ProxyShell and ProxyNotShell.

A variation of ProxyNotShell was exploited in the ransomware

attack targeting cloud company Rackspace.

Despite warnings and high-profile incidents, many organizations fail to install patches, providing attackers with tens of thousands of potential targets to choose from.

Exchange Server 2013 reached end of support three months after Windows 7 Extended Security Updates (ESU) and Windows 8.1 reached their end of support dates.

Related: Microsoft: No-Interaction Outlook Zero Day Exploited Since Last April

Related: Microsoft Urges Customers to Patch Exchange Servers

Related: Microsoft Confirms Exploitation of Two Exchange Server Zero-Days

Microsoft Exchange Server 2013 Reaches End of Support