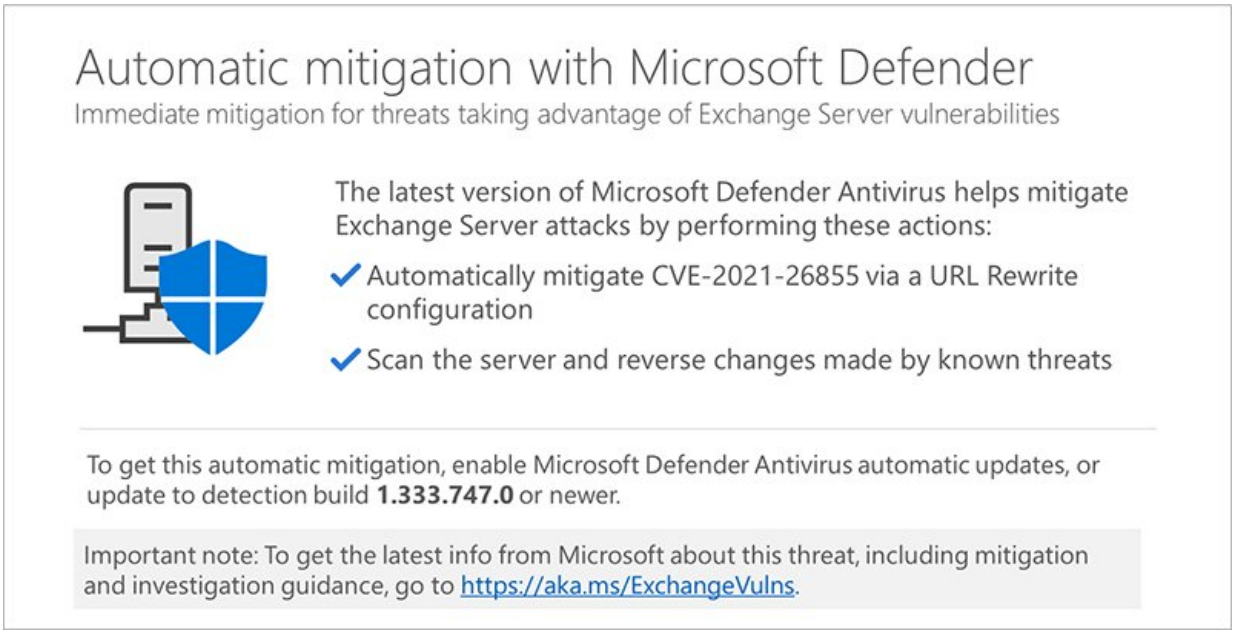
Microsoft Defender Antivirus now offers automatic on-premises Exchange Server mitigation

March 22 2021, by Sarah Katz



Microsoft Exchange Server On-Premises Mitigation Tool. Credit: Microsoft

In light of the plethora of cybercriminals who have attempted to attack unpatched on-premises versions of Exchange Server 2013, 2016 and 2019, Microsoft has ramped up its support of customers and partners in securing their environments and responding to related incidents.

So far, the company has introduced a comprehensive Security Update, a detailed guide to help address these attacks and a single-click interim Exchange On-Premises Mitigation Tool for both current and out-of-support versions of on-premises Exchange Servers. The Security Update involves recommendation to begin remediation by updating any Exchange Servers connected to or published on the Internet, as attackers have been exploiting HTTPS Web access.

For customers who have yet to implement this upgrade and so remain at risk, Microsoft has released a security intelligence update including Microsoft Defender Antivirus and System Center Endpoint Protection that will automatically defend against this threat, CVE-2021-26855, on any affected vulnerable Exchange Server. To activate this functionality, customers should either turn on automatic updates or simply install the latest security intelligence update 1.333.747.0.

In fact, this security update offers users time to implement the latest Exchange Cumulative Update for their version of Exchange. Additionally, Microsoft intends to collaborate with its security partners so they may apply similar mitigations for their own products.

For Microsoft customers who might be wondering whether the automatic definition updates default setting is enough to cover this change, they only have to make sure to install Microsoft Defender Antivirus. At this point, the customer will be able to select and add the new detection build 1.333.747.0, or higher.

That said, customers should still make sure that security updates are a continued top priority for their Exchange Server, as many vulnerabilities may still emerge. Fortunately, however, in the meantime, Microsoft will automatically detect vulnerable installed Exchange Servers and apply all mitigations as soon as the customer deploys the security intelligence update. Each impacted machine will receive this mitigation.

Furthermore, while cloud protection is not required to obtain this mitigation, such protection is always a helpful security measure to protect both company and user assets against all of the dynamic cyber threats out there. Therefore, Microsoft encourages customers to enable cloud protection for whichever type of cloud environment their company uses.

Finally, customers who do not yet have Microsoft Defender Antivirus can begin by downloading the One-Click Microsoft Exchange On-Premises Mitigation Tool and immediately running the tool on their Exchange servers. For those already using Microsoft Safety Scanner, this tool and the Mitigation Tool can be used in unison.

More information: "Automatic on-Premises Exchange Server Mitigation Now in Microsoft Defender Antivirus." Microsoft Security, Microsoft, 19 Mar. 2021, www.microsoft.com/security/blo … -defender-antivirus/