One-Click Microsoft Exchange On-Premises Mitigation Tool – March 2021

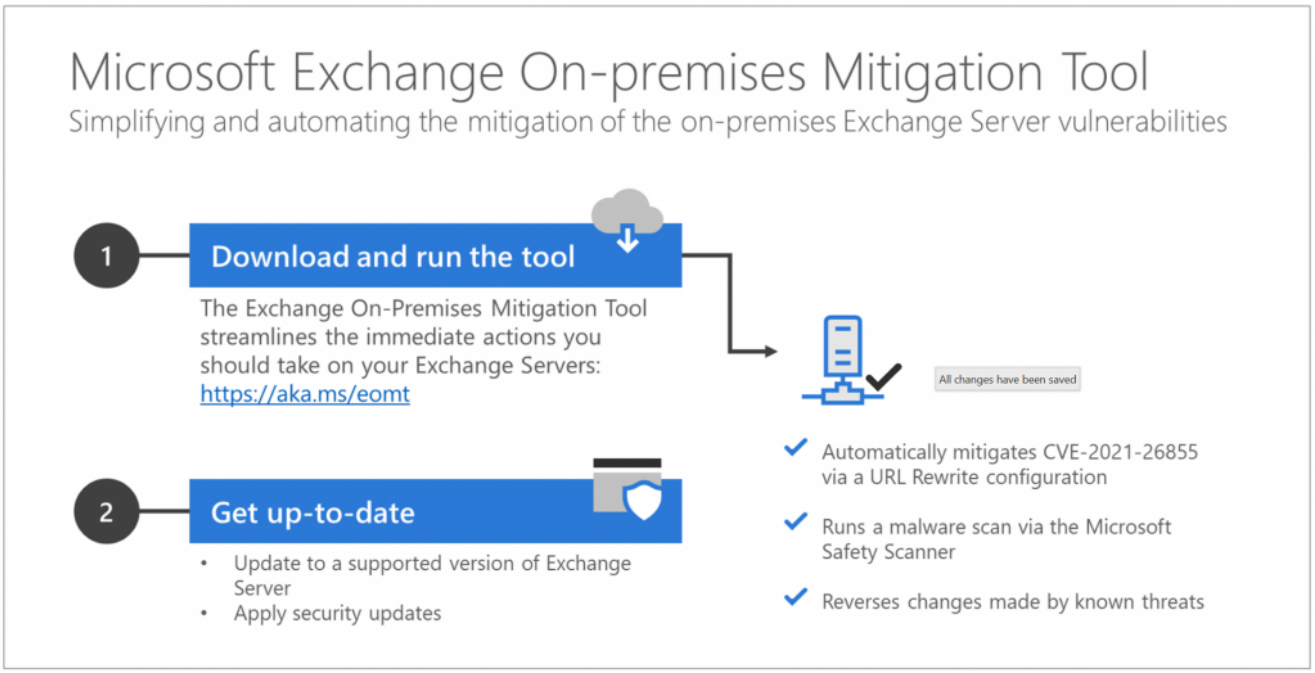

msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/

We have been actively working with customers through our customer support teams, third-party hosters, and partner network to help them secure their environments and respond to associated threats from the recent Exchange Server on-premises attacks. Based on these engagements we realized that there was a need for a simple, easy to use, automated solution that would meet the needs of customers using both current and out-of-support versions of on-premises Exchange Server.

Microsoft has released a new, one-click mitigation tool, Microsoft Exchange On-Premises Mitigation Tool to help customers who do not have dedicated security or IT teams to apply these security updates. We have tested this tool across Exchange Server 2013, 2016, and 2019 deployments. This new tool is designed as an interim mitigation for customers who are unfamiliar with the patch/update process or who have not yet applied the on-premises Exchange security update.

By downloading and running this tool, which includes the latest Microsoft Safety Scanner, customers will automatically mitigate CVE-2021-26855 on any Exchange server on which it is deployed. This tool is not a replacement for the Exchange security update but is the fastest and easiest way to mitigate the highest risks to internet-connected, on-premises Exchange Servers prior to patching.
We recommend that all customers who have not yet applied the on-premises Exchange security update:

- Download this tool.
- Run it on your Exchange servers immediately.
- Then, follow the more detailed guidance here to ensure that your on-premises Exchange is protected.
- If you are already using Microsoft Safety Scanner, it is still live and we recommend keeping this running as it can be used to help with additional mitigations.



Once run, the Run EOMT.ps1 tool will perform three operations:

Mitigate against current known attacks using CVE-2021-26855 using a URL Rewrite configuration.
Scan the Exchange Server using the Microsoft Safety Scanner.
Attempt to reverse any changes made by identified threats.

Before running the tool, you should understand:

- The Exchange On-premises Mitigation Tool is effective against the attacks we have seen so far, but is not guaranteed to mitigate all possible future attack techniques. **This tool should only be used as a temporary mitigation until your Exchange servers can be fully updated as outlined in our previous guidance.**
- **We recommend this script over the previous ExchangeMitigations.ps1 script as it tuned based on the latest threat intelligence.** If you have already started with the other script, it is fine to switch to this one.
- This is a recommended approach for Exchange deployments with Internet access and for those who want to attempt automated remediation.
- Thus far, we have not observed any impact to Exchange Server functionality when these mitigation methods are deployed.

For more technical information, examples, and guidance please review the GitHub documentation.

Microsoft is committed to helping customers and will continue to offer guidance and updates that can be found at https://aka.ms/exchangevulns.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS GUIDANCE. The Exchange On-premises Mitigation Tool is available through the MIT License, as indicated in the GitHub Repository where it is offered.