What is the purpose of this notification?

This notification provides guidance for customers regarding new security updates released by Microsoft to resolve privately reported security vulnerabilities that affect Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019. We are releasing updates for Exchange Server 2010 for defense-in-depth purposes.

Recommend Actions

- Microsoft recommends placing a high priority on deploying the March security updates to address these critical security vulnerabilities.
- Priority should be given to Internet-facing Exchange servers, which are at increased risk.
- Please factor in extra servicing time for any Exchange servers that are not running a currently supported Update Rollup (UR) or Cumulative Update (CU). Any Exchange servers that are not up to date will need to have a supported UR or CU installed before you can install any new security updates.
- Please review the webpages at the links in this alert for more information about these security vulnerabilities, recommended actions, and links to download the security updates.

Answers to Anticipated Questions

Q: Do these vulnerabilities affect Exchange Online?

A: No. Customers using Exchange Online are not affected by these vulnerabilities.

Q: What is the maximum severity, impact, and Base CVSS score of these vulnerabilities?

A: The set of vulnerabilities include Remote Code Execution vulnerabilities that have a severity rating of critical. The highest base CVSS score in the set is 9.1.

Q: Were vulnerabilities affecting Exchange Server known to have been exploited in the wild?

A: Yes. Microsoft is aware of limited targeted attacks against on-premises Exchange servers by a nation-state actor that leveraged four of the Exchange vulnerabilities discussed on this release.

Q: How many Exchange Server vulnerabilities are being fixed in this release?

A: The security update release contains fixes for seven security vulnerabilities affecting Exchange Server. Of these, four vulnerabilities were known to have been used in limited, targeted attacks against on-premises Exchange servers.

Q: Do I need to do any prep work with my Exchange servers to make them ready for these new security updates?

A: Microsoft provides support for the latest two Cumulative Updates (CUs) for Exchange Server 2016 and Exchange Server 2019. Microsoft provides support for the latest Update Rollup (UR) for Exchange Server 2010 and Exchange Server 2013. Exchange servers running a supported UR or CU are considered up to date. Any Exchange servers that are not up to date will need to have a supported UR or CU installed before you can install any new security updates. Exchange administrators should factor in additional time needed to update out-of-date Exchange servers.

Q: Is there a method I can use to determine which of my Exchange servers can install the security updates directly, and which will need to have a supported UR or CU installed first?

A: Yes. You can use the Exchange Server Health Checker script, which can be downloaded from GitHub (use the latest release). Running this script will tell you if you are behind on your on-premises Exchange Server updates.

Q: Do I need to prioritize specific Exchange servers (are some Exchange servers at increased risk)?

A: Yes. Internet-facing Exchange servers (*e.g.*, servers publishing Outlook on the web/OWA and ECP) are at an increased risk and these should be updated first. Your servicing plan should include identifying and prioritizing Internet-facing Exchange servers.

Q: Are there workarounds for these vulnerabilities?

A: These vulnerabilities are used as part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443. This can be protected against by restricting untrusted connections, or by setting up a VPN to separate the Exchange server from external access. Using this mitigation will only protect against the initial portion of the attack; other portions of the chain can be triggered if an attacker already has access or can convince an administrator to run a malicious file.

Q: How can I check to identify if any of my Exchange servers have been compromised by any of these vulnerabilities?

A: The Microsoft Threat Intelligence Center (MSTIC) blog post referenced below provides technical guidance that security specialists can use to hunt for intrusions that may have involved any of these vulnerabilities.

Q: Were these vulnerabilities affecting Exchange Server related to recent attacks impacting SolarWinds?

A: No. We are not aware of any connection between these vulnerabilities affecting Exchange Server and the recent attacks impacting SolarWinds.

Q: Where can I find the most authoritative information about these Exchange Server vulnerabilities?

A: The best resources for technical details on the vulnerabilities are the CVE pages and the MSTIC blog post referenced below.

Security Vulnerability Details

CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability				
Impact	Remote Code Execution	Base CVSS Score	9.1	Scope	Unchanged
Severity	Critical	Attack Vector	Network	Confidentiality	High
Publicly Disclosed?	No	Attack Complexity	Low	Integrity	High
Known Exploits?	Yes	Privileges Required	None	Availability	None
Exploitability	Exploitation detected	User Interaction	None	Release Date	March 9, 2021
Affected Software	Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019				
More Information	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855				

CVE-2021-26857	Microsoft Exchange Server Remote Code Execution Vulnerability				
Impact	Remote Code Execution	Base CVSS Score	7.8	Scope	Unchanged
Severity	Critical	Attack Vector	Local	Confidentiality	High
Publicly Disclosed?	No	Attack Complexity	Low	Integrity	High
Known Exploits?	Yes	Privileges Required	None	Availability	High
Exploitability	Exploitation detected	User Interaction	Required	Release Date	March 9, 2021
Affected Software	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019				
More Information	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857				

CVE-2021-26858	Microsoft Exchange Server Remote Code Execution Vulnerability				
Impact	Remote Code Execution	Base CVSS Score	7.8	Scope	Unchanged
Severity	Important	Attack Vector	Local	Confidentiality	High
Publicly Disclosed?	No	Attack Complexity	Low	Integrity	High
Known Exploits?	Yes	Privileges Required	None	Availability	High
Exploitability	Exploitation detected	User Interaction	Required	Release Date	March 9, 2021
Affected Software	Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019				
More Information	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858				

CVE-2021-27065	Microsoft Exchange Server Remote Code Execution Vulnerability				
Impact	Remote Code Execution	Base CVSS Score	7.8	Scope	Unchanged
Severity	Critical	Attack Vector	Local	Confidentiality	High
Publicly Disclosed?	No	Attack Complexity	Low	Integrity	High
Known Exploits?	Yes	Privileges Required	None	Availability	High
Exploitability	Exploitation detected	User Interaction	Required	Release Date	March 9, 2021
Affected Software	Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019				
More Information	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065				

Related Resources

- Exchange Team Blog: https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
- MSRC blog: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server
- MSTIC blog: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- On the Issues (MOTI) blog: https://blogs.microsoft.com/on-the-issues/?p=64505

- CVE-2021-26855 | Microsoft Exchange Server Remote Code Execution Vulnerability: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

- CVE-2021-26857 | Microsoft Exchange Server Remote Code Execution Vulnerability: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857

- CVE-2021-26858 | Microsoft Exchange Server Remote Code Execution Vulnerability: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858

- CVE-2021-27065 | Microsoft Exchange Server Remote Code Execution Vulnerability: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

- The Security Update Guide: http://aka.ms/securityupdateguide

Regarding Information Consistency

We strive to provide you with accurate information in static (this mail) and dynamic (web-based) content. Microsoft's security content posted to the web is occasionally updated to reflect late-breaking information. If this results in an inconsistency between the information here and the information in Microsoft's web-based security content, the information in Microsoft's web-based security content is authoritative.

If you have any questions regarding this alert, please contact your Customer Success Account Manager (CSAM).

Thank you.