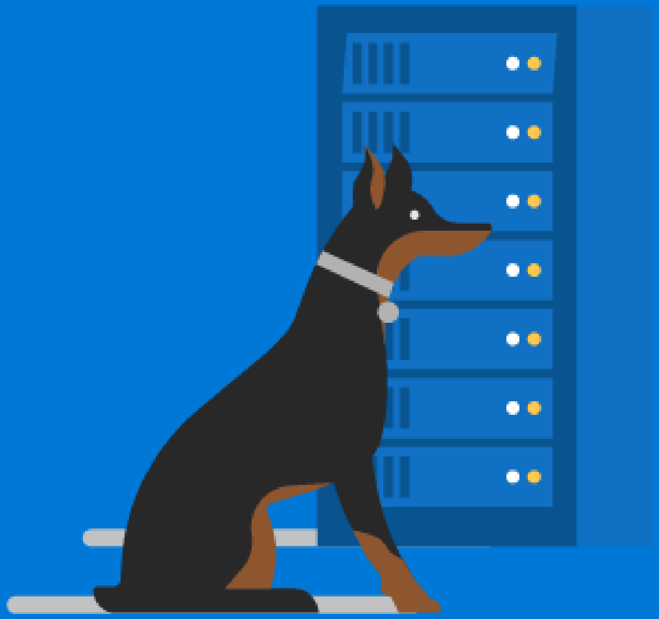
Microsoft

Microsoft EMEA Exchange Server Out of Band

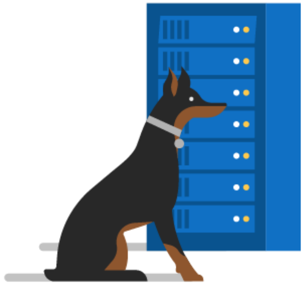
18 March, 2021

Get the deck at https://aka.ms/ExOOB



Elizabeth Tyler CCSK
Microsoft EMEA Security Program Manager
Twitter: @MSEtyler

March 2, 2021 - Exchange Server Out of Band Key Info.



Affects Exchange Server on-premises ONLY, Exchange Online unaffected. If you have hybrid, you have at least one on-premises Exchange Server and it needs to be patched:

- Exchange Server 2013
- Exchange Server 2016
- Exchange Server 2019
- Exchange Server 2010 is out of support but is being updated for Defense-in-Depth purposes. The attack targets 2013/2016/2019 (*free*)

Is there anything I need to do before installing this update?

***UPDATE**: Fixes for older CU's are now available* [March 2021 Exchange Server Security Updates for older Cumulative Updates]()

However* 1) This fix is for 4 exploited vulnerabilities only, not all 7. You will still need to be at these versions to be supported:

- Exchange Server 2010 (RU 31 for Service Pack 3 – this is a Defense-in-Depth update)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

How critical is this?

Prioritize installing updates on Exchange Servers that are externally facing such as your OWA servers. All affected Exchange Servers should ultimately be updated.

How can I tell if my servers have already been compromised?

Information on Indicators of Compromise (IOCs) – such as what to search for, and how to find evidence of successful exploitation (if it happened), can be found in [HAFNIUM Targeting Exchange Servers]()

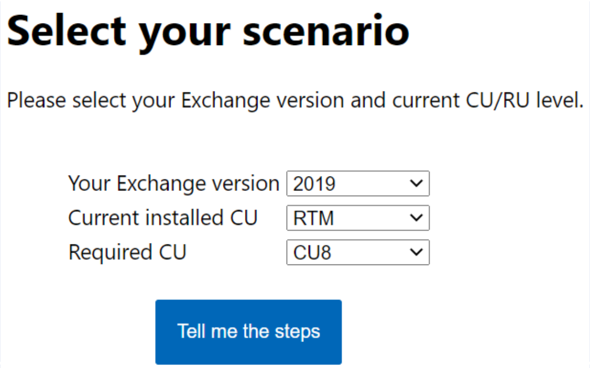
Where are the download links?

They are at the [Security Update Guide]() and at [Multiple Security Updates Released for Exchange Server – Microsoft Security Response Center]()

Microsoft

One click Mitigation tool	One-Click Microsoft Exchange On-Premises Mitigation Tool – March 2021 – Microsoft Security Response Center
MSRC blog updated 16 March	https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server
MSTIC blog – Most Detailed:	https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
Guidance for Responders blog	Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities – Microsoft Security Response Center
Mitigation Tool	One-Click Microsoft Exchange On-Premises Mitigation Tool *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.*
Depending on what CU you are migrating from you may also need:	.NET upgrade guidance - .NET Framework 4.7 and Exchange Server - Microsoft Tech Community Schema update information - Active Directory schema changes in Exchange Server | Microsoft Docs

*N



Select your scenario

Please select your Exchange version and current CU/RU level.

Your Exchange version: 2019

Current installed CU: RTM

Required CU: CU8

Run Safety Scanner in detect-only mode Microsoft Safety Scanner, this is standalone Defender. D/L a fresh copy before each time you run for the latest sigs. Safety Scanner *ignores* exclusions so can be better than normal AV

Kevin Beaumont @GossiTheDog · 1h

Four chained zero days are being exploited in the wild against Exchange Server, aka Outlook Web App.

Patches available now, action required to apply

Full remote code execution, without authentication.

Exchange Server team script to run a check for HAFNIUM IOCs https://github.com/microsoft/CSS-Exchange/tree/main/Security

Repair failed installations of Exchange Cumulative and Security updates
Issues due to Exchange Updates

For finding out CU level and if the patch successfully applied: GitHub - dpaulson45/HealthChecker: Exchange Server Performance Health Checker Script

Exchange Engineers Tech Help FAQ: Troubleshooting Guide from Exchange Engineers

Some Cumulative Update (CU) Best Practices

- Backup any and all customizations. They will not survive the update
- Reboot the server beforehand
- Remember certain CUs require AD Schema and/or .NET Framework updates. See slide 3
- Enable Maintenance Mode
- Use an elevated command prompt to run the CU.
- Temporarily disable any anti-virus software during the update process.
- Reboot your server upon completion of the update.
- Disable Maintenance Mode

Overview - Exchange RCE Vulnerabilities

- Exchange 2013, 2016, 2019
- Targeted attacks detected
- Part of an attack chain
- Initial attack over Exchange port 443
- Exchange Online is not affected

Recommended Actions

Apply security updates

Microsoft provides support for the two latest CUs for each supported Exchange Server version. Exchange servers running a supported UR or CU are considered up to date. Any Exchange servers that are not up to date will need a supported UR or CU installed before you can install these new security updates. Exchange administrators should factor in the additional time needed for any out-of-date Exchange servers. Exchange administrators can run a Health Checker script to determine the status of each Exchange server.

Check environment for signs of compromise

1. Scan Exchange logs for IOC
2. Check hosts for IOC: web shell hashes, known paths and filenames, LSASS process memory dumps

Reference
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Defender Protections

Microsoft Defender Antivirus

Exploit:Script/Exmann.A!dha
Behavior:Win32/Exmann.A
Backdoor:ASP/SecChecker.A
Backdoor:JS/Webshell (not unique)
Trojan:JS/Chopper!dha (not unique)
Behavior:Win32/DumpLsass.A!attk (not unique)
Backdoor:HTML/TwoFaceVar.B (not unique)

Microsoft Defender for Endpoint Protections

Suspicious Exchange UM process creation
Suspicious Exchange UM file creation
Possible web shell installation (not unique)
Process memory dump (not unique)

Azure Sentinel and Advanced Hunting

Azure Sentinel Detections

HAFNIUM Suspicious Exchange Request
HAFNIUM UM Service writing suspicious file.
HAFNIUM New UM Service Child Process
HAFNIUM Suspicious IM Service Errors
HAFNIUM Suspicious File Downloads

Advanced Hunting Queries

Microsoft Defender for Endpoint: https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/
Azure Sentinel: https://github.com/Azure/Azure-Sentinel/tree/master/Detections/MultipleDataSources/

Exchange FAQ – also see FAQ for March 2021 Exchange Server Security Updates - Microsoft Q&A

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..*

Microsoft