

Gina Johnson

From: Gina Johnson
Sent: Tuesday, March 9, 2021 11:31 AM
To: Gina Johnson
Subject: RE: INTENDED FOR WIDEST DISTRIBUTION: Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities

WARNs - PLEASE SEE ADVISORY BELOW

From: "Sector.Partnership" <Sector.Partnership@cisa.dhs.gov>
Date: March 5, 2021 at 10:49:17 PM EST
Subject: Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities

Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities

INTENDED FOR WIDEST DISTRIBUTION

Critical Infrastructure Colleagues and Partners,

The Cybersecurity and Infrastructure Security Agency (CISA) strongly urges its partners to follow guidance provided to Federal Civilian Executive Branch Departments and Agencies at cisa.gov/ed2102. This CISA Emergency Directive outlines key steps federal officials must take to immediately address this vulnerability. **We cannot stress enough the seriousness of this vulnerability; it is widespread and is indiscriminate.**

As a follow up to the conference call CISA held earlier today regarding the Microsoft Exchange widespread vulnerability affecting on-premise deployments, CISA published this evening the following [Current Activity](#) supplemental guidance to ensure all partners understand the severity of the vulnerability and steps to detect and mitigate potential compromise. All information surrounding this vulnerability can also be found directly at www.cisa.gov.

NOTE: Exploitation of this vulnerability before patch installation permits an adversary to gain persistent access to and control of entire enterprise networks which is likely to persist even after patching.

Please immediately speak with your IT officials to determine what steps your organization has taken, and if your organization does not have the technical capability to verify network integrity please consider bringing in a third party to assist you as soon as possible.

Everyone using Microsoft Exchange on-premise products must:

Check for signs of compromise;

Immediately patch Microsoft Exchange with the vendor released patch;

If unable to patch, remove the products from the network immediately; and

Upgrade to the latest supported version of Microsoft Exchange.

Response to indicators of compromise are essential to eradicate adversaries already on your network and must be accomplished in conjunction with measures to secure the Microsoft Exchange

environment. Patching an already compromised system will not be sufficient to mitigate this situation; therefore, CISA strongly encourages partners to immediately disconnect any Microsoft Exchange systems suspected of being compromised.

Please contact CISA for any questions or to report an incident regarding this vulnerability at Central@cisa.gov.

----- **Actions for IT Admins/Staff** -----

CISA is tracking a serious issue with Microsoft Exchange. We cannot emphasize enough that exploitation is widespread and indiscriminate and we are advising all system owners to complete the following actions.

Please follow the ensuing checklist and provide feedback to your leadership on the actions you have taken and any challenges completing the recommended steps.

- o [Patch](#) ALL instances of Microsoft Exchange that you are hosting.
- o If you can't patch then follow the recommendations Microsoft issued -- [Microsoft Exchange Server Vulnerabilities Mitigations – March 2021 – Microsoft Security Response Center](#) .
- o Check for indicators of compromise by running the following [script](#) .
- o If you haven't been compromised we strongly recommend enhance monitoring of network connections to your Exchange environment.
- o If you have, follow this [guidance](#) to better understand what to do next.

Respectfully,

Cybersecurity and Infrastructure Security Agency
Defend Today Secure Tomorrow



This communication is the property of the American Water Works Association and may contain confidential or privileged information. Unauthorized use of this communication is strictly prohibited and may be unlawful. If you have received this communication in error, please immediately notify the sender by reply email and destroy all copies of the communication and any attachments.

American Water Works Association
Dedicated to the World's Most Important Resource ®