High-Severity Vulnerability in Hybrid Microsoft Exchange Deployments

The U.S. EPA is issuing this alert to inform water and wastewater system owners and operators about a newly disclosed high-severity vulnerability that could allow a cyber threat actor to move laterally from Microsoft Exchange servers hosted and operated on-site (commonly referred to as "on-premises") to the Microsoft 365 cloud environment. Although the exploitation of this vulnerability is only possible after an attacker establishes administrative access on the on-premises Microsoft Exchange server, this vulnerability poses a grave risk to all water and wastewater systems operating Microsoft Exchange hybrid (onsite and cloud) joined configurations and immediate mitigation is critical. The Cybersecurity and Infrastructure Security Agency (CISA) has issued a cybersecurity alert on this malicious activity.

Mitigations

All drinking water and wastewater systems with Microsoft Exchange hybrid-joined environments are strongly encouraged to implement the following mitigations immediately to enhance resilience against this compromise:

- **First, inventory all Microsoft Exchange Servers on your network(s) to confirm if there are any Microsoft Exchange hybrid configurations on the network(s) (utilities are encouraged to use existing visibility tools or publicly available tools, such as Network Mapper (NMAP) or PowerShell scripts, to accomplish this task).**
- **If using Microsoft Exchange hybrid configuration, review Microsoft's guidance Exchange Server Security Changes for Hybrid Deployments to determine if your Microsoft hybrid deployments are potentially affected.**
- **Install Microsoft's April 2025 Exchange Server Hotfix Updates on the on-premise Exchange server and follow Microsoft's configuration instructions: Deploy dedicated Exchange hybrid app.**
- **For organizations using Exchange hybrid (or have previously configured Exchange hybrid but no longer use it), review Microsoft's Service Principal Clean-Up Mode.**
- **Upon completion, run the Microsoft Exchange Health Checker to determine if further steps are required.**
- **Consider disconnecting public-facing versions of Microsoft Exchange Server or SharePoint Server that have reached their end-of-life (EOL) or end-of-service from the internet.**

For additional information on this vulnerability, drinking water and wastewater systems owners and operators are encouraged to review Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments.

Conclusion

The U.S. EPA requests that the Water Sector Coordinating Council (WSCC)/Government Coordinating Council (GCC) review this advisory and pass it along to all water & wastewater entities that may be susceptible to this threat. Additionally, we encourage the EPA Regions to share the advisory with the state primacy agencies and direct implementation utilities.

Water and wastewater system owners and operators should direct their IT/OT system administrators to review this alert for further use and implementation. If you rely on third party vendors for technology support, then you are encouraged to contact them to confirm their awareness of this threat. Organizations are encouraged to report information concerning suspicious or criminal activity to FBI Internet Crime Complaint Center (IC3) at IC3.gov or to CISA via CISA's Incident Reporting System. If you have questions about any of the information contained in this document, please contact the Water Infrastructure and Cyber Resilience Division, Cybersecurity Branch at watercyberta@epa.gov.