Active Exploitation of Microsoft SharePoint Vulnerabilities

The U.S. EPA is issuing this alert to inform water and wastewater system owners and operators about the active exploitation of security vulnerabilities in Microsoft SharePoint that allows attackers to mislead the system into thinking they are a trusted user, also known as network spoofing, and remotely run malicious code, known as a remote code execution (RCE). This exploit enables unauthorized access specifically to Microsoft SharePoint servers, which are hosted and operated on-site. The Cybersecurity and Infrastructure Security Agency (CISA) has issued a cybersecurity alert on this malicious activity, publicly reported as "ToolShell."

Mitigations

All drinking water and wastewater systems with Microsoft SharePoint servers are strongly encouraged to implement the following mitigations immediately to enhance resilience against this compromise:

- **Apply the necessary security updates released by Microsoft.**
- **Configure Antimalware Scan Interface (AMSI) in SharePoint and deploy Microsoft Defender Antivirus on all SharePoint servers.**
- **Rotate ASP.NET machine keys, then after applying Microsoft's security update, rotate ASP.NET machine keys again, and restart the Internet Information Services (IIS) web server.**
- **Disconnect public-facing versions of SharePoint Server that have reached their end-of-life (EOL) or end-of-service (EOS) from the internet.**
- **Conduct scanning for IPs 107.191.58[.]76, 104.238.159[.]149, and 96.9.125[.]147, particularly between July 18-19, 2025.**
- **Monitor for malicious POST requests to** ***/_layouts/15/ToolPane.aspx?DisplayMode=Edit***
- **Update intrusion prevention system and web application firewall rules to block exploit patterns and anomalous behavior.**
- **Implement comprehensive logging to identify exploitation activity.**
- **Audit and minimize layout and admin privileges.**

For additional information on detection, prevention, and advanced threat hunting measures, drinking water and wastewater systems owners and operators are encouraged to visit Microsoft's Disrupting active exploitation of on-premises SharePoint vulnerabilities and advisory as well as CISA's cybersecurity alert.

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 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.