



TLP:CLEAR

Identify and Mitigate Potential Compromise of Cisco Devices

The United States Environmental Protection Agency (EPA) is issuing this alert to inform water and wastewater systems about Emergency Directive (ED) 25-03 issued by the Cybersecurity and Infrastructure Security Agency (CISA). This directive highlights an ongoing exploitation campaign by an advanced threat actor targeting Cisco Adaptive Security Appliances (ASA). The campaign is widespread and involves exploiting zero-day vulnerabilities to achieve unauthenticated remote code execution on Cisco ASAs. Additionally, it includes the manipulation of read-only memory (ROM), enabling threat actors to maintain access even through reboots and system upgrades.

Link to Emergency Directive 25-03: <https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices>

Mitigations

Although Emergency Directive 25-03 is directed at federal agencies, EPA strongly recommends that water and wastewater systems review the Emergency Directive and follow the mitigation steps. The Emergency Directive includes a detailed step-by-step guide along with resources to assist in implementing each mitigation. Systems that outsource technology support should consult with their service providers for assistance with these steps.

Important: Water and wastewater systems are not required to report their activities to CISA, including those outlined in mitigation steps 2, 3, and 6 in the Emergency Directive. This requirement applies only to federal agencies; however, systems may choose to report voluntarily and are encouraged to do so if a compromise is detected.

Conclusion

If you have questions about any of the information in this alert, including assistance with the mitigation steps included in the Emergency Directive, please submit a request to [EPA's Cybersecurity Technical Assistance Program for the Water Sector](#).

Additionally, CISA has provided the following contact information specific to this Emergency Directive:

- General information, assistance, and reporting: CyberDirectives@cisa.dhs.gov
- Reporting indications of compromise: contact@cisa.dhs.gov