TLP:CLEAR

Mitigate Vulnerabilities in F5 Devices

The United States Environmental Protection Agency (EPA) is issuing this alert to inform water and wastewater systems about Emergency Directive (ED) 26-01 issued by the Cybersecurity and Infrastructure Security Agency (CISA).

This directive highlights an ongoing exploitation campaign by a nation-state affiliated cyber threat actor that has compromised F5 systems. The actor has exfiltrated data, including portions of F5's BIG-IP source code and vulnerability information, providing them with a technical advantage to exploit F5 devices and software. This poses a critical threat to water and wastewater systems using F5 products. F5 is a is a technology company that provides products and services to protect and enhance the speed, reliability, and security of applications and networks.

- Link to Emergency Directive 26-01: https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices
- Specific Common Vulnerability and Exposure (CVE) information can be found on the vendor's webpage: https://my.f5.com/manage/s/article/K000156572

Mitigations

Although Emergency Directive 26-01 is directed at federal agencies, EPA strongly recommends that water and wastewater systems review the Emergency Directive and follow the mitigation steps. 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.b, 6, and 8 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