TLP:CLEAR

Security Vulnerability Affecting FortiWeb Products

The U.S. EPA is issuing this alert to inform water and wastewater system owners and operators about the active exploitation of a newly disclosed vulnerability in Fortinet FortiWeb (a web application firewall). The vulnerability, tracked as CVE-2025-64446, is a relative path traversal security flaw that allows a remote, unauthenticated attacker to execute administrative commands on a vulnerable system. This vulnerability affects the following FortiWeb versions:

- 8.0.0 through 8.0.1
- 7.6.0 through 7.6.4
- 7.4.0 through 7.4.9
- 7.2.0 through 7.2.11
- 7.0.0 through 7.0.11

Mitigations

All drinking water and wastewater systems running the affected FortiWeb versions are strongly encouraged to implement the following mitigations immediately to enhance resilience against this compromise. Systems that outsource technology support should consult with their service providers for assistance with these steps:

- Apply the necessary upgrades listed in the table below.

Version	Affected	Solution
FortiWeb 8.0	8.0.0 through 8.0.1	Upgrade to 8.0.2 or above
FortiWeb 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
FortiWeb 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
FortiWeb 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiWeb 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.12 or above

- If you cannot immediately upgrade the affected systems, disable HTTP or HTTPS for internet-facing interfaces. Note: Limiting access to HTTP/HTTPS

management interfaces to internal networks is a best practice that reduces, but does not eliminate, risk; upgrading the affected systems remains essential and is the only way to fully remediate this vulnerability.

- After upgrading, review configuration and review logs for unexpected modifications or the addition of unauthorized administrator accounts. It's recommended to review and test all upgrades to ensure the upgrades do not negatively impact operations.

Conclusion

For additional details please refer to the CISA alert and Fortinet's mitigation guidance. If you have questions about any of the information in this alert, including assistance with the mitigation steps, please submit a request to EPA's Cybersecurity Technical Assistance Program for the Water Sector.

Additionally, CISA requests that organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at contact@cisa.dhs.gov or (888) 282-0870.