

Fortinet Critical Security Updates

Date: October 22, 2026

Across the technology industry, organizations are responding to newly identified cybersecurity vulnerabilities, prompting widespread security updates and accelerated patching efforts.

Fortinet has announced critical security updates affecting several of its products, including FortiGate firewalls. Twin State Technical Services (TSTS) is taking immediate action to address these security risks for our customers.

Protecting our customers is our highest priority. We are treating these updates with urgency and taking proactive steps to address identified vulnerabilities as quickly and safely as possible.

Thank you for your continued trust in Twin State Technical Services.

What's Happening

On **October 22, 2026**, Fortinet is scheduled to release updates for critical and high-severity vulnerabilities affecting **FortiOS, FortiManager, and FortiAnalyzer**.

These vulnerabilities could expose affected network security systems to unauthorized access or other cyberattacks if left unpatched.

Fortinet recommends applying the updates **immediately** rather than waiting for a routine maintenance window.

What TSTS Is Doing

For customers with TSTS-managed Fortinet equipment, our team is preparing to:

- Identify affected devices and review current firmware versions.
- Apply security updates as soon as fixes are available, without waiting for regularly scheduled maintenance.
- Verify each update and confirm that affected systems are operating properly.

What This Means for Your Business

TSTS is reviewing managed Fortinet environments to determine what action is needed.

Once the patches are released, we anticipate completing updates for nearly all affected managed environments within 36 hours of patch availability.

Required updates are urgent, and maintenance may need to be scheduled on short notice. We will perform updates after hours whenever possible. If a service interruption is necessary, our team will coordinate with affected customers and work to minimize disruption.

Please note:

- Not all customers or Fortinet devices are affected.
- We are sharing this advisory with all TSTS customers as a proactive security notice.
- Receiving this notice does not necessarily mean your organization is affected.
- If no remediation is required for your environment, you may not receive further communication regarding this advisory.

What This Means for Internet or Network Connectivity

If your device is affected, the firewall update may briefly interrupt internet access, VPN connections, or other network-dependent services. **The expected interruption is approximately 15–30 minutes.**

What Action Should I Take

TSTS-managed customers

There is no need to take any action or submit a service request. Our team is proactively coordinating these updates. If we contact you regarding urgent maintenance, **please respond promptly** so we can complete the necessary work without delay.

Self-managed or Co-managed customers

If TSTS is not responsible for managing your Fortinet equipment, please ensure your IT team is aware of these vulnerabilities and **takes immediate action**. If you are unsure who is responsible for these updates, contact TSTS for assistance.

Where to Find Updates

For additional information, please review **[Fortinet's Official Security Announcement, October 21, 2026](#)**.