Urgent Security Alert: Cisco Secure Firewall Adaptive Security Appliance Software and Cisco Secure Firewall Threat Defense Software

The Southcentral CMS QIN-QIO (Region 5) is notifying healthcare organizations of a high-severity vulnerability (CVE-2026-76418) affecting Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software.

Cisco has released security updates for CVE-2026-76418, a high-severity vulnerability affecting the VPN service in certain Cisco firewall products. An external attacker could exploit this vulnerability without a valid username or password and cause an affected firewall to restart unexpectedly. This could temporarily interrupt remote access and other services that rely on the device.

Cisco reported active exploitation of this vulnerability in October 2026. Because affected firewalls may support important business operations, organizations should promptly determine whether they use these products and apply the available security updates.

Organizations should refer to the Cisco vendor security advisory for affected versions, fixed versions, configuration details, and upgrade guidance.

Why this matters to your organization

- **Active exploitation:** Cisco has reported that attackers are actively exploiting this vulnerability.
- **No credentials required:** An external attacker may be able to exploit the vulnerability without a valid username or password.
- **Potential impact:** A successful attack could cause an affected firewall to restart, temporarily disrupting remote access and other business services that depend on the device.

Recommended actions

Please ensure your internal IT team or Managed Service Provider (MSP) completes the following steps immediately:

- **Determine exposure:** Confirm whether your organization uses Cisco Secure Firewall ASA or FTD products and whether the affected remote access feature is enabled.
- **Review vendor guidance:** Refer to the Cisco vendor security advisory for affected versions, fixed versions, configuration details and upgrade guidance.
- **Apply available updates:** Upgrade affected systems to a fixed version as soon as possible, following Cisco's recommendations.
- **Review temporary mitigation options:** If an update cannot be applied immediately, ask your IT team or MSP to review Cisco's documented mitigation. Cisco cautions that the mitigation may affect system functionality or reduce the security provided by secondary authentication.
- **Prioritize exposed systems:** Give priority to affected firewalls that provide remote access or can be reached from the internet.

Continued

Learn more

- Cisco Security Advisory
- New Cisco firewall zero-day exploited to crash SSL VPN devices
- CISA Adds Two Known Exploited Vulnerabilities to Catalog
- National Institute of Standards and Technology National Vulnerability Database

This material was prepared by TMF Health Quality Institute, the Quality Innovation Network-Quality Improvement Organization, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents do not necessarily reflect CMS policy. 13SOW-QINQIO-GEN-26-282 11/2026