Cisco patches ASA and FTD zero-day exploited to crash firewalls



Cisco has released updates for a denial-of-service zero-day in ASA and Threat Defense (FTD) software. Attackers are already exploiting it to remotely crash vulnerable firewall devices, including SSL VPN services.

- The flaw is a denial-of-service zero-day in Cisco Adaptive Security Appliance (ASA) and Threat Defense (FTD) software.
- Attackers are actively exploiting it to remotely crash vulnerable firewall devices.
- Cisco has released security updates to fix the issue.
- The headline indicates SSL VPN devices are among those being crashed.
- The excerpt provided does not include CVE details or affected version lists, so check Cisco's advisory.

Cisco has issued security updates for a zero-day vulnerability in its Adaptive Security Appliance (ASA) and Threat Defense (FTD) software. The flaw allows denial of service, and attackers are already using it to remotely crash vulnerable firewall devices.

What is known

The issue was exploited before a fix was available, which is why it is classed as a zero-day. According to the report, the impact is that affected firewalls can be forced to fail remotely, and the headline specifically refers to SSL VPN devices being crashed. The excerpt available to us does not give a CVE identifier, affected versions or technical conditions for exploitation.

Why it matters

Firewalls and VPN gateways sit at the network edge. If they are crashed repeatedly, remote access for staff and partners can be interrupted, and perimeter protection may be lost until the device recovers. For regulated institutions this is an availability and business continuity concern as much as a security one.

Recommended approach

Treat this as a priority patching item for any ASA or FTD deployment. Confirm exposure using Cisco's official advisory, which will list the affected releases and fixed versions, and plan the update through your normal emergency change process. Meanwhile, watch for unexpected reloads or crashes of firewall devices, as these may indicate attempted exploitation.

What to do now

1. Inventory all Cisco ASA and FTD devices, including those serving SSL VPN, and record their software versions.
2. Review Cisco's official advisory for affected and fixed releases, and schedule the update as an emergency change.
3. Monitor firewall logs and device health for unexpected crashes or reloads and investigate any found.
4. Confirm failover or high-availability and alternative remote access arrangements work in case a gateway goes down.
5. Report confirmed exploitation or service disruption through your incident process and, where required, to the relevant regulator.