Cisco Firewall DoS Vulnerability in IKEv2 Affects ASA, FTD, IOS, and IOS XE

TL;DR

A denial-of-service vulnerability (CVE-2026-20012, CVSS 8.6) in Cisco IKEv2 could allow an unauthenticated attacker to crash or destabilize devices by sending crafted packets.

Successful exploitation can force device reloads or exhaust memory. It can also disrupt VPN access and network availability. There are no workarounds.

Overview

There is a vulnerability (CVE-2026-20012, CVSS 8.6) in Cisco's Internet Key Exchange version 2 (IKEv2) feature affecting IOS, IOS XE, and Cisco firewall platforms, including Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD). The issue comes from improper parsing of IKEv2 packets, which allows an unauthenticated remote attacker to send crafted traffic that triggers a memory leak.

Affected Products

- Cisco IOS Software
- Cisco IOS XE Software
- Cisco Secure Firewall ASA Software
- Cisco Secure Firewall Threat Defense (FTD) Software

Note: (Only systems with IKEv2 enabled are impacted.)

On firewall devices, this directly impacts VPN availability and stability. An attacker can exhaust system memory, prevent new VPN sessions from forming, or cause the device to become unstable until it is manually rebooted. Remote users may lose access, site-to-site tunnels can drop, and security controls tied to the firewall may stop working as expected.

For an organization, this can lead to loss of secure remote access and gaps in network visibility. If a firewall becomes unstable during business hours, it can interrupt key services and leave parts of the network exposed while systems recover. Aspire recommends patching CVE-2026-20012 immediately.

Aspire Protects

- **Patch** - Apply Cisco security updates immediately. See Cisco's advisory for more information.
- Identify devices with IKEv2 enabled and prioritize them for patching.
- Monitor for unexpected device reloads or VPN instability.
- Restrict unnecessary exposure of IKEv2 services to untrusted networks.
- Review VPN configurations and disable IKEv2 where not required.

TTPs to Watch

Impact

- Endpoint Denial of Service [T1499] – The attacker may send crafted IKEv2 packets to exhaust memory or force device reloads, disrupting network availability.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using VPN-based connectivity or Cisco network infrastructure are most exposed, including:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability