PACKETVIPER®

Firewall Vendor Zero-Days in 2026: What They Reveal, and Where a Preemptive Layer Changes the Outcome

Six actively-exploited perimeter vendor CVEs in 2026, read against PacketViper's preemptive, agentless architecture.

COMPETITIVE & MARKET PERSPECTIVE

What's inside

Six 2026 zero-days across Palo Alto Networks, Fortinet, Check Point, and Cisco — what happened, and how PacketViper's stated architecture (AMTD, agentless inline enforcement, Hive-mind propagation, behavioral trust modeling) is positioned to change the outcome for this category of exposure.

Prepared July 14, 2026

Why This Matters

Over the past several months, five of the industry's best-known perimeter security vendors — Palo Alto Networks, Fortinet, Check Point, Cisco, and SonicWall — have each disclosed critical, actively-exploited zero-day vulnerabilities in their firewall, VPN, or SD-WAN products. These are not obscure or theoretical flaws: several carry CVSS scores above 9.0, several were exploited before a patch existed, and at least two are tied to known ransomware operations. CISA has repeatedly added these CVEs to its Known Exploited Vulnerabilities catalog and, in one case, gave federal agencies a three-day emergency patch window.

The pattern across all six incidents below is consistent: the firewall or VPN appliance is the trust boundary and the single point of enforcement, so a flaw in its authentication or management logic doesn't just create a hole — it hands the attacker the keys to everything the device was supposed to protect. Below, each incident is summarized on its own, followed by a look at how PacketViper's stated architecture — an inline, agentless, preemptive layer that sits alongside (not in place of) the firewall — is positioned to address that category of exposure.

A note on how to read this

These are commentary and analysis, not independent test results. Where PacketViper has not been validated against a specific CVE, that is noted rather than implied.

The Six Incidents

1. Palo Alto Networks PAN-OS — Unauthenticated Root RCE (CVE-2026-0300)

A critical buffer overflow in the User-ID Authentication Portal service of PAN-OS allows an unauthenticated remote attacker to execute arbitrary code with root privileges on PA-Series and VM-Series firewalls. Rated 9.3 out of 10, the flaw has reportedly been exploited since at least April 2026 by a likely state-sponsored actor, and CISA added it to its Known Exploited Vulnerabilities catalog.

Source: Hackers run code on PAN-OS firewalls as root without authentication — cybernews.com

HOW PACKETVIPER ADDRESSES THIS

This is exactly the failure mode PacketViper's own homepage leads with: a static, rule-based control point is a single point of compromise once its own authentication logic breaks. PacketViper's model doesn't rely on the firewall's internal trust boundary at all — it sits inline as an agentless Layer 2 bridge and evaluates every connection attempt to a protected service (including the firewall's own management and portal interfaces) against behavioral and contextual signals: source reputation, geography, and reconnaissance patterns. An unauthenticated exploit attempt against a portal service typically looks, from the wire, like anomalous probing before it looks like a valid session — the exact reconnaissance phase PacketViper's Automated Moving Target Defense (AMTD) and Global Network Lists are built to catch and block before the exploit payload is ever delivered.

2. Palo Alto Networks GlobalProtect — VPN Authentication Bypass (CVE-2026-0257)

An authentication bypass in the GlobalProtect portal and gateway let attackers skip login entirely and establish an unauthorized VPN session. Palo Alto initially rated it medium severity; within four days of public disclosure, active exploitation was confirmed and the rating was raised to critical.

Source: Hackers are exploiting Palo Alto GlobalProtect VPN authentication bypass — Help Net Security

HOW PACKETVIPER ADDRESSES THIS

The four-day gap between disclosure and mass exploitation is the window PacketViper is designed to operate in without needing a CVE number at all. Because its enforcement is based on live behavior rather than a signature for this specific bypass, an attacker establishing a VPN session it has no prior trust relationship for — from an unexpected geography, at an unusual time, with no preceding legitimate handshake — is the kind of deviation PacketViper's contextual filtering and trust modeling are built to flag or stop outright, independent of whether the underlying authentication logic in the VPN gateway itself was sound that day.

3. Fortinet FortiClient EMS — Authentication Bypass to Full RCE (CVE-2026-35616)

An improper access control flaw in the FortiClient EMS API let attackers send crafted requests to bypass authentication and authorization entirely, achieving code execution on the underlying server with no credentials and no user interaction. Independent researchers detected active exploitation days before Fortinet's own advisory was published — a true zero-day. CISA added it to its Known Exploited Vulnerabilities catalog within two days of disclosure.

Source: Fortinet FortiClient EMS Zero-Day: CVE-2026-35616 — watchTowr

HOW PACKETVIPER ADDRESSES THIS

This is a management-plane API being hit directly — precisely the kind of narrow, high-value target that PacketViper's Asset Management and passive discovery are meant to keep continuously mapped and watched, and that AMTD is meant to keep from being reliably found or fingerprinted in the first place. PacketViper's own positioning is direct on this point: a network that doesn't change is a network that can be fully mapped and catalogued for later use. An EMS API sitting at a static, discoverable address is exactly the kind of asset AMTD is designed to make unreliable to locate and fingerprint from outside the trust boundary.

4. Fortinet FortiCloud SSO — Auth Bypass on Fully Patched Firewalls (CVE-2026-24858)

Multiple Fortinet customers reported attackers creating new local administrator accounts on FortiGate firewalls that were already running the latest FortiOS updates. The flaw allowed any attacker with a FortiCloud account and a registered device to bypass authentication and reach other devices tied to different customer accounts when SSO was enabled — meaning being fully patched provided no protection on its own.

Source: Fortinet's latest zero-day vulnerability carries frustrating familiarities for customers — CyberScoop

HOW PACKETVIPER ADDRESSES THIS

This is the clearest case for behavior- and trust-based enforcement over patch status alone. PacketViper's site describes exactly this scenario as a design target: it models expected trust relationships between assets, and "anything outside the pattern gets stopped — not flagged." A brand-new local admin account appearing on a firewall, or an unfamiliar device suddenly reaching that firewall's management plane through an SSO relationship it has never used before, is a deviation from established behavior that this model is intended to catch — regardless of whether the specific CVE enabling it is known, patched, or even disclosed yet.

5. Check Point — VPN/Mobile Access Zero-Day Tied to Qilin Ransomware (CVE-2026-50751)

A critical authentication bypass affecting Check Point Remote Access VPN, Mobile Access, and Spark Firewall products (CVSS 9.3) was found being actively exploited, with post-exploitation activity retrieving malicious payloads from attacker-controlled infrastructure and ties identified to the Qilin ransomware operation. CISA gave federal agencies a three-day window to patch.

Source: Critical Check Point VPN Zero-Day Exploited in the Wild — Rapid7

HOW PACKETVIPER ADDRESSES THIS

This case shows why the moment of initial compromise matters more than the speed of the eventual patch — a three-day patch window is still three days of exposure across an entire fleet. PacketViper's "Hive" architecture is built around that gap: when any single unit detects malicious behavior, it blocks locally and propagates that block to every other unit across the enterprise in milliseconds, without waiting on a human to push a policy. Applied to a scenario like this one, a VPN endpoint compromised at one site would not, on its own, need to be independently rediscovered and blocked at every other site before containment took effect.

6. Cisco — Sixth SD-WAN Zero-Day of 2026, Plus Continued ASA/FTD Exploitation

Cisco patched its sixth actively-exploited SD-WAN zero-day disclosed in 2026 alone, this one tied to a sophisticated actor tracked as UAT-8616. Separately, Cisco has continued to warn of ongoing attacks against its ASA and FTD firewall lines, including a vulnerability the Interlock ransomware group exploited as a zero-day for months before disclosure. As of July 2026, 93 Cisco CVEs sit on CISA's Known Exploited Vulnerabilities catalog.

Source: Cisco Patches Another SD-WAN Zero-Day, the Sixth Exploited in 2026 — SecurityWeek

HOW PACKETVIPER ADDRESSES THIS

Six exploited zero-days in a single product line in a single year is a volume problem as much as a vulnerability problem — every one of them requires its own detection signature, its own patch cycle, and its own confirmation that no prior exploitation occurred. PacketViper's pitch is explicitly that it doesn't need to know what a given exploit looks like in advance: its enforcement operates on reconnaissance and behavioral deviation, which is present before almost any exploit attempt, rather than on a growing library of vulnerability-specific signatures. That doesn't reduce Cisco's patch burden, but it is intended to shrink the window in which an unpatched device can be found and hit in the first place.

The Common Thread

Every incident above shares the same shape: a device whose entire job is to be the trust boundary had a flaw in the logic that decides who to trust, and the blast radius was the device's full privileges — root code execution, a forged admin account, an unauthorized VPN session, a foothold for ransomware. None of these were exotic attacks; several were found and exploited faster than the vendor could patch.

PacketViper's own positioning, as stated on packetviper.com, is built around treating that pattern as the baseline threat model rather than the exception:

- Agentless, inline enforcement — sits in the traffic path around the firewall/VPN appliance rather than depending on that appliance's own internal logic being sound.
- AMTD (Automated Moving Target Defense) — continuously shifts the network's visible attack surface so the reconnaissance that typically precedes exploitation of a management or VPN portal returns unreliable results.
- Behavioral/trust modeling — flags or blocks activity (a new admin account, an unfamiliar device, an unexpected session) that deviates from established patterns, independent of whether a specific CVE is known or patched yet.
- Hive-mind propagation — a block detected at one site or unit is pushed to every other unit in the deployment in milliseconds, narrowing the window between first detection and full containment.
- Global Network Lists — automatic filtering by country, business entity, and threat category before a packet is even evaluated against the protected service.

A compensating control, not a patch replacement

None of this argues against patching — it argues for not relying on patch cycles alone. Every incident above shares the same exposure window: the gap between when a flaw exists and when it is found, disclosed, and fixed, a gap AI-accelerated reconnaissance and exploitation are compressing every year. A compensating control is built to hold that window closed. Because PacketViper enforces on behavior and reconnaissance rather than a signature for a specific CVE, it does not need to know these six vulnerabilities in advance to add a layer of defense-in-depth against the pattern they represent. That is the fit worth testing directly — PacketViper offers a proof-of-concept against a real environment as a standard option (packetviper.com/proof-of-concept).

Sources

- Hackers run code on PAN-OS firewalls as root without authentication: critical zero-day unveiled — Cybernews
- Hackers are exploiting Palo Alto GlobalProtect VPN authentication bypass (CVE-2026-0257) — Help Net Security
- Fortinet FortiClient EMS Zero-Day: CVE-2026-35616 (Active Exploitation Underway) — watchTowr
- Fortinet's latest zero-day vulnerability carries frustrating familiarities for customers — CyberScoop
- Critical Check Point VPN Zero-Day Exploited in the Wild (CVE-2026-50751) — Rapid7
- Cisco Patches Another SD-WAN Zero-Day, the Sixth Exploited in 2026 — SecurityWeek
- PacketViper — Preemptive Network Security for IT & OT (homepage, capabilities, FAQ)

About PacketViper

PacketViper delivers Preemptive cybersecurity and Automated Moving Target Defense solutions for OT/ICS and IT practitioners in critical infrastructure industries seeking real-time visibility into their environment's expanding attack surface. Our patented technology allows users to proactively defend OT/ICS assets, remote OT endpoints, and IT infrastructures. PacketViper's agentless detection, prevention, containment, deception, and response technology automates attack detection and prevention from both external and internal threats. Our solutions provide operators with the contextual security data required to act quickly while potential threats are still in motion, and before critical OT/ICS and IT assets are compromised.