CISO's Vulnerability Remediation Playbook Series

Immediate remediation guidance on Chrome Zero-Days, AMD Zen 5 Flaw, Control Web Panel RCE, and Critical Cisco Exploits

What you will get inside

- Detailed breakdown of each critical vulnerability
- The risks and potential business impact they pose
- Clear mapping between exploit severity and response priority.
- Temporary mitigations you can deploy
- Remediation actions

Actionable steps to prevent direct exploitation

Why These Vulnerabilities Demand Immediate Action

The recent wave of critical vulnerabilities across browsers, hardware, and network infrastructure has revealed a new reality, attackers exploit faster than organizations can patch.

Zero-day exploitation

Google Chrome's zero-day (CVE-2025-2783) was actively exploited by the ForumTroll APT group to deploy LeetAgent spyware. This campaign shows how attackers are weaponizing common applications instantly, bypassing traditional detection windows and exploiting end-user trust.

Browser exploit chains

Chrome's recurring V8 engine vulnerabilities (CVE-2025-12428, CVE-2025-12429) enable remote code execution through drive-by exploitation. The persistence of type confusion flaws proves that JavaScript engines remain a favored and reliable attack vector for sophisticated threat actors.

Network control layers attacks

The Cisco ISE RADIUS vulnerability (CVE-2025-20343) enables attackers to trigger repeated restarts and cause denial-of-service conditions by abusing failed authentication loops. When exploited, it disrupts network visibility, authentication, and compliance enforcement, making remediation a top operational priority.

Hardware threats

The AMD Zen 5 RDSEED flaw (CVE-2025-62626) compromises the integrity of hardware-based random number generation, weakening encryption and secure boot. By targeting the CPU's entropy source, attackers can corrupt cryptographic trust at its root, turning hardware into a persistent point of failure.

Web infrastructure exploits

A command injection vulnerability in Control Web Panel (CVE-2025-48703) is under active exploitation, allowing unauthenticated remote code execution. This flaw has resulted in complete server compromise across hosting environments, underscoring the urgency of patching critical internet-facing systems immediately.

Neutralization of Firewalls

Active exploitation of Cisco ASA and FTD vulnerabilities (CVE-2025-20333, CVE-2025-20362) demonstrates how attackers are neutralizing firewalls through memory corruption and authorization bypass flaws. Compromised devices can expose internal networks and degrade defense-in-depth architectur

Remediate these critical vulnerabilities faster with SecPod's Saner Platform, powered by Unified Security Intelligence

Know these vulnerabilities & remediate them using Saner

CVE ID / Vulnerability	Affected Products	Exploitability	Remediation Steps	How to remediate using Saner
CVE-2025-2783 – Google Chrome Zero-Day Sandbox Escape (LeetAgent Spyware)	Google Chrome (Windows, macOS, Linux) before 134.0.6998.177; Chromium-based browsers	Actively exploited by APT ForumTroll in "Operation ForumTroll" espionage campaign	✓ Update Chrome to 134.0.6998.177+ ✓ Enable Enhanced Safe Browsing ✓ Block phishing links and untrusted extensions	Detect systems with outdated Chrome, deploy the latest update, and confirm patching automatically using Saner
CVE-2025-62626 – AMD Zen 5 RDSEED Hardware Entropy Flaw	AMD EPYC 9005, Ryzen 9000, Ryzen AI, Ryzen HX processors	Locally exploitable by privileged users; impacts cryptographic trust and secure boot integrity	✓ Apply AMD AGESA TurinPI 1.0.0.8+ firmware updates ✓ Use 64-bit RDSEED variant only ✓ Regenerate cryptographic keys created during exposure ✓ Disable RDSEED temporarily (clearcpuid=rdseed)	Detect affected AMD systems, apply firmware or BIOS updates, and track patch completion status
CVE-2025-48703 – Control Web Panel Command Injection	Control Web Panel (CWP) before 0.9.8.1182	Under active exploitation; allows unauthenticated remote code execution	✓ Upgrade CWP to 0.9.8.1182+ immediately ✓ Restrict access to the admin panel via firewall/VPN ✓ Rotate credentials and apply WAF filtering ✓ Include CWP patch in server maintenance automation	Locate servers running old CWP versions, upgrade to the secure release, and validate patch update with Saner
CVE-2025-20343 – Cisco ISE RADIUS DoS Vulnerability	Cisco Identity Services Engine (ISE) RADIUS Service	Remotely exploitable; triggers repeated RADIUS restarts causing DoS	✓ Update Cisco ISE to patched release ✓ Rate-limit RADIUS authentication attempts ✓ Segment RADIUS traffic for resilience ✓ Validate configuration compliance using SanerNow	Detect affected ISE appliances, apply the vendor patch, and check patch compliance using Saner
CVE-2025-20333 / CVE-2025-20362 – Cisco ASA & FTD Firewall Memory Corruption and Auth Bypass	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) platforms	Actively exploited to gain admin access or crash firewalls	✓ Upgrade ASA/FTD to latest firmware	Detect impacted ASA/FTD devices, update to the latest firmware, and confirm successful patching through Saner

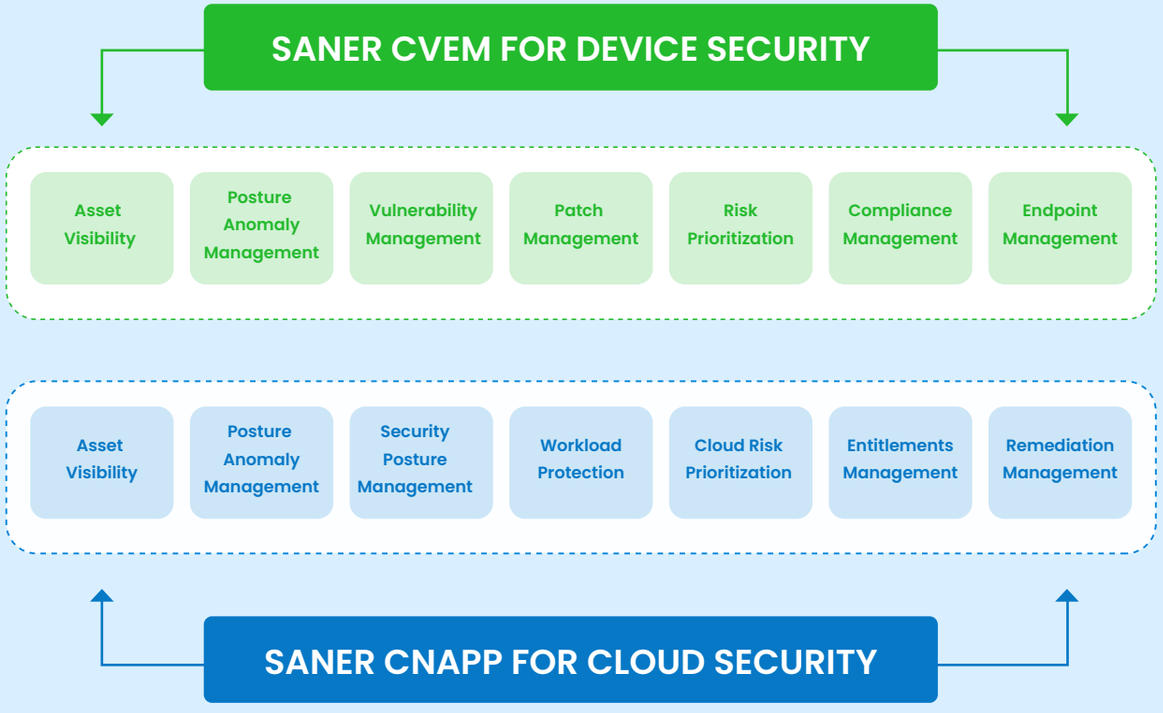
All vulnerabilities can be automatically discovered, prioritized, remediated, and verified through SecPod's Saner Platform, ensuring faster remediation & measurable risk reduction.

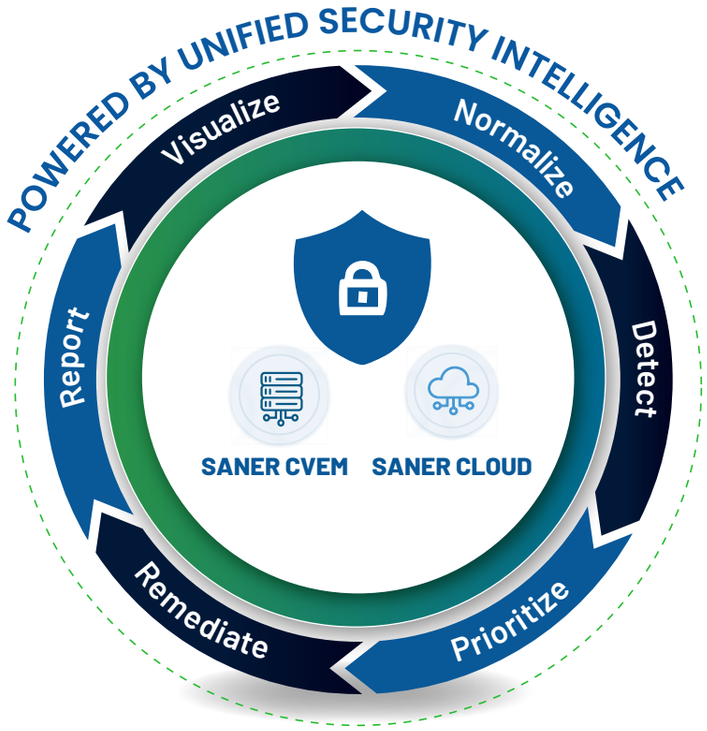
About Saner Platform

SecPod's Saner is an integrated, proactive, vulnerability management platform that can scan, normalize, prioritize, and remediate endpoints and cloud assets.

Unified Security Intelligence forms the platform's core. It brings together vulnerability data from across the IT infrastructure to surface weaponized exposures, map attack paths, prioritize remediation and stop compromise.

This ensures faster SLA driven remediation of weaknesses and fewer blind spots across the attack surface.





SANER CVEM FOR DEVICE SECURITY

SANER CNAPP FOR CLOUD SECURITY

SecPod's Saner is an integrated, proactive, vulnerability management platform that can scan, normalize, prioritize, and remediate endpoints and cloud assets.

Unified Security Intelligence forms the platform's core. It brings together vulnerability data from across the IT infrastructure to surface weaponized exposures, map attack paths, prioritize remediation and stop compromise.

This ensures faster SLA driven remediation of weaknesses and fewer blind spots across the attack surface.

Know more about Saner's Patch Management Capabilities

About SecPod

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure every connected computing device across modern enterprises by delivering preventive, automated, and intelligent cybersecurity.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture and prevent cyberattacks before they strike.

The platform includes:

Cloud Security

An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.

Vulnerability & Exposure Management

A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.

Endpoint and Patch Management

A Continuous Risk Remediation solution that minimizes the attack surface by eliminating potential risks across the IT infrastructure.

With its suite of cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

Visit us www.secpod.com
Write to us info@secpod.com

Connect with us