

Cyber Advisories & Patch Reference

Active vulnerabilities, confirmed exploitation, and remediation priority · Updated Sep 19, 2026

Patch Priority — In Order

#	What	Severity	Why it comes here
1	Linux kernels — CVE-2025-39682, CVE-2025-39964, CVE-2026-53266	CRITICAL	Federal deadline Mon Sep 21. Active exploitation confirmed. Linux runs most cloud, server and industrial systems
2	Orkes Conductor — CVE-2026-58138	CRITICAL	Pre-authentication remote code execution, CVSS 9.8. Exploited in the wild. Update past 3.30.2
3	Check Point Security Management / Log Servers	CRITICAL	Remote code execution as root on the perimeter management console
4	WordPress — "Click2Shell"	HIGH	A crafted link forces a theme install and chains to code execution. Enormous install base
5	ABB Ability Edgenius — CVE-2026-31431	HIGH	Compromised container workload can gain root on industrial edge systems. Update to 3.2.4.1 or later
6	Google Chrome — KEV entry added Sep 18	HIGH	Confirmed exploitation. Every desktop. Relaunch to apply
7	Unbound DNS resolver — CVE-2026-81642	HIGH	Heap overflow in the DNSSEC validator; remote code execution via a malicious zone. Verify version 1.26.1 or later

Active Exploitation List — Extended

Product / Flaw	Severity	Status and notes
Cisco Identity Services Engine — CVE-2026-76460	CVSS 10.0	Unauthenticated remote authentication bypass. The network's identity gatekeeper
Cisco Secure Email Gateway — CVE-2026-76461	HIGH	Root command execution. Actively exploited
Acronis cPanel/WHM Backup plugin — CVE-2026-87886	CVSS 7.8	Local privilege escalation via insecure file permissions. Targeted attacks; shared-hosting customers inherit the risk
Microsoft Azure AI Foundry — CVE-2026-85889	CVSS 10.0	Missing authentication allowed unauthenticated network privilege escalation. Server-side fix; Microsoft states no customer action required
ConnectWise ScreenConnect · JFrog Artifactory (two flaws) · GitLab path traversal · MikroTik RouterOS · Google Pixel modem (CVE-2026-58704)	HIGH	All on the Known Exploited Vulnerabilities list with confirmed in-the-wild use

AI Coding Agent Supply Chain

"Plugin4Shell." A repository owner can swap a version-pinned plugin for malicious code across four widely used AI coding agents — even when the version is locked.

Patched: Claude Code 2.1.179 (Anthropic) · Codex 0.146.0 (OpenAI).

Unpatched at last report: GitHub Copilot.

Impact: direct software supply-chain risk for any development team using AI agents.

Supply Chain & Credential Incidents

Incident	Detail and lesson
TanStack npm attack → ~170 private GitHub repositories	An attacker used a departed employee's still-active GitHub access ; that employee's laptop had been compromised in the May TanStack npm attack. Lesson: revoke access the day someone leaves, and audit what your dependencies can reach
Abandoned CDN domain re-registered	Thousands of sites, repositories and documents still hard-code hostnames beneath a domain whose CDN was wound down years ago. The new owner controls what those sites load
Gyazo image-upload service breach	Approximately 23 million user records compromised via a server vulnerability
Transparent Tribe (Pakistan-aligned)	New Rust backdoor family with private GitHub repositories used for command and control . Targets government and defense entities in India and Afghanistan

Permanently Unpatchable

Mitsubishi Electric CC-Link IE TSN (CVE-2026-13584) — denial of service across a wide range of MELSEC controllers. CISA's advisory was updated Sep 17 to add newly affected models, and states **"no fix planned"** for some of them. If you operate this equipment, the remedy is **network segmentation**, not patching. Treat the control network as hostile-by-default.

Standing Sources

- CISA Known Exploited Vulnerabilities catalog — cisa.gov/known-exploited-vulnerabilities-catalog
- CISA cybersecurity advisories feed — cisa.gov/cybersecurity-advisories/all.xml
- Report an incident — cisa.gov/report
- The Hacker News — thehackernews.com · SecurityWeek — securityweek.com/feed · Krebs — krebsonsecurity.com/feed
- Foreign CERTs worth reading the same day: ENISA (EU) · NCSC (UK) · BSI (Germany) · JPCERT (Japan) · ACSC (Australia) · CERT-EU