CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- North Carolina Ports, the US authority operating the ports of Wilmington, Morehead City and others, has suffered a cyberattack that forced some operations onto manual processes. The authority claims it has contained the intrusion, but degraded systems caused delays while affected services were restored.
- Ryde, an electric scooter operator in Scandinavian countries, has disclosed a data breach affecting all 4.5 million customer accounts across Norway, Sweden, Finland, and Germany. Attackers copied phone numbers, email addresses, birth dates, partial payment card numbers, and payment histories. Full card numbers and ride histories were unaffected.
- Canadian hardware wallet maker Coinkite has disclosed a theft campaign exploiting a Coldcard firmware vulnerability, with at least 1,367 bitcoin worth about $88.6 million stolen from thousands of addresses. The company halted affected shipments, destroyed vulnerable inventory, and released patched firmware after confirming exploitation against customer wallets.
- Beacon, a UK provider of customer relationship management software for charities, has disclosed a data breach after attackers compromised an access key. The company notified around 1,500 nonprofit customers that database information, donation records, and stored attachments may have been downloaded. Payment and bank details were not affected.

AI THREATS

- Check Point Research has demonstrated that Cloudflare Code Mode, which allows AI agents to write TypeScript against tools, inherited five vulnerabilities from the workerd runtime. The flaws could enable sandbox escape and cross-tenant data exposure. Cloudflare rated two issues Critical and fixed its managed Workers environment.
- Researchers have disclosed vulnerabilities in Google Gemini CLI and Anthropic Claude Code that could expose automation environments to code execution and API key theft. CVE-2026-12537, rated CVSS 10.0, affected Gemini CLI workflows, while CVE-2026-54316 affected Claude Code. Both vendors released patched versions.
- Researchers have detailed AI-enabled identity fraud kits that automate know-your-customer bypasses across banks, fintech companies, and cryptocurrency exchanges. Tools such as ProKYC can generate identity documents, selfie-with-ID images, spoofed location data, and synthetic video used against document, selfie, and liveness checks during remote onboarding.

VULNERABILITIES AND PATCHES

- Cisco has released fixes for multiple critical vulnerabilities in Catalyst SD-WAN and IOS XE software disclosed on August 5. The highest-severity issues carry CVSS scores up to 9.9 and can enable privilege escalation, code execution, or system compromise. Cisco also addressed additional high and medium-severity flaws across network management products.
- WordPress has released version 7.0.3 to address CVE-2026-64638, a high-severity Core vulnerability known as XSS2Shell. The flaw can turn a failed login into pre-authentication cross-site scripting and, under specific conditions, remote code execution. Fixes were also backported for supported WordPress branches dating to version 4.7.
- TP-Link has addressed 15 vulnerabilities in its Omada provisioning ecosystem affecting controllers, network devices, mobile applications, and VIGI cameras. The flaws include device impersonation, credential exposure, and remote code execution risks during provisioning. 11 flaws received CVE identifiers, and patched firmware has been released for affected products.
- A vendor-installed backdoor has been identified across at least 20 Zbtlink router models sold under brands including Wiflyer and ZBT. The remote-management component contacts hardcoded servers and can accept unauthenticated commands with root privileges. Researchers reproduced the behavior by impersonating the vendor server and obtaining a root shell.

THREAT INTELLIGENCE REPORTS

- Researchers have identified the Shai-Hulud CHAINDROP supply-chain campaign, which backdoored more than 400 npm packages after attackers compromised the maintainer of the widely used keyv library. The malware executes through a preinstall hook, steals developer tokens, and republishes modified packages, affecting an ecosystem with roughly 1.3 billion monthly downloads.
- Researchers have uncovered a campaign targeting large US financial firms in which callers impersonate coworkers or IT staff to capture passwords and multi-factor authentication codes through spoofed websites. The actors, tracked as UNC6671, then threaten victims with data leaks and have issued ransom demands ranging from $750,000 to $3 million.
- Researchers have revealed a macOS ClickFix campaign using more than 250 look-alike domains to distribute MacSync and Atomic Stealer malware. The operation evolved to fingerprint visitors before displaying malicious instructions, allowing attackers to target genuine macOS users while concealing the campaign from automated security scanners and analysis systems.
- Researchers have documented a campaign that uploaded nearly 800 malicious npm packages delivering cross-platform RAT and infostealer malware. The packages instructed developers to import them, activating the WEL1DROPPER downloader. It retrieved payloads through Cloudflare Workers or DNS TXT records, established persistence, and deployed additional malicious tools.