CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The European Commission, the European Union's executive body, has confirmed a data breach after its Europa.eu platform was compromised through a third-party exchange linked to the Trivy supply chain attack. The incident affected at least one Amazon Web Services account and resulted in data theft, while websites and internal systems remained operational.
- Global toys and games manufacturing giant Hasbro has disclosed a cyberattack after detecting unauthorized access to its network on March 28. Some systems were taken offline, and the company warned that recovery could take weeks and cause delays.
- Cryptocurrency trading platform Drift Protocol on Solana has suffered a major breach after an attacker gained enough Security Council approvals to execute pre-signed transactions on April 1. Drift said roughly $280 million was affected, froze platform activity, and stated the incident did not involve a smart contract flaw or seed phrase compromise.
- Luxury camping providers Roan and Eurocamp have experienced a data breach that exposed guest names, email addresses, phone numbers, travel destinations, booking dates, and prices. Attackers are using the stolen data in WhatsApp payment scams, while the companies said the flaw was patched and no passwords or payment data were taken.

AI THREATS

- Check Point Research demonstrated a hidden outbound channel in ChatGPT’s execution runtime that enabled silent exfiltration of user data. A single malicious prompt or a backdoored GPT could transmit chat content and uploaded files to attackers through DNS.
- Check Point warns that based on leaked details about Anthropic’s Claude “Mythos”, the model will likely accelerate vulnerability discovery, exploit development, and multi-step attack automation. The new capabilities could sharply reduce time to exploit and make advanced offensive techniques more broadly accessible.
- Researchers examined six AI agents and found that impersonation and fabricated urgency can push them to disclose data or take harmful actions. In testing, an agent forwarded 124 emails containing personal and financial details, while others deleted files and reassigned admin access.
- Researchers observed a flaw in Google Cloud's Vertex AI Agent Engine that could let attackers extract service agent credentials and pivot into customer projects. The exposed privileges enabled access to storage and Artifact Registry resources, and permissive OAuth scopes also increased the risk of wider Google Workspace exposure.

VULNERABILITIES AND PATCHES

- Cisco released urgent fixes for CVE-2026-20093, a critical authentication bypass in its Integrated Management Controller software used across ENCS 5000, Catalyst 8300 uCPE, and UCS C-Series M5 and M6 servers. Remote attackers can reset any account, including Admin, allowing full device takeover.
- Researchers discovered CVE-2026-5281, a zero-day memory flaw in Chrome's WebGPU component, Dawn, that also impacts Edge, Brave, Opera, and other Chromium-based browsers. The vulnerability is being actively exploited and can enable code execution on user systems, prompting inclusion in CISA's Known Exploited Vulnerabilities catalog.
- Progress has addressed two critical ShareFile vulnerabilities, including CVE-2026-2699 with a CVSS score of 9.8, that can be chained for unauthenticated remote code execution. The flaws let attackers reach restricted configuration pages and upload arbitrary files to the server without logging in to affected installations.
- F5 reclassified CVE-2025-53521, a BIG-IP Access Policy Manager vulnerability, as a critical remote code execution flaw under active exploitation. More than 14,000 internet-exposed systems were still visible online, and the company published indicators of compromise and rebuild guidance for affected devices.

THREAT INTELLIGENCE REPORTS

- Check Point Research has unmasked TrueChaos, a campaign exploiting a 0-day vulnerability (CVE-2026-3502) in TrueConf's on-premises update process to push malicious updates to Southeast Asian government networks. Attackers delivered Havoc payloads through trusted servers, and the activity was assessed with moderate confidence as being affiliated with a Chinese nexus.
- Check Point Research have outlined an Iran-nexus password-spraying campaign against Microsoft 365 in the Middle East, conducted in three waves during March. The activity focused on Israel and the UAE, targeting municipalities and using Tor and VPN infrastructure to evade geofencing and complicate attribution.
- Check Point Research have uncovered coordinated tax-season phishing and malware activity, with hundreds of newly registered tax-themed domains and rising risk levels. In March 2026, one in ten new domains was flagged as risky, while IRS-impersonating sites harvested personal data and Spain-themed emails delivered malware loaders.
- Researchers documented a supply chain compromise of the Axios npm package, a widely used HTTP client with millions of monthly downloads, that briefly pushed malicious releases delivering a remote access trojan. The tampered versions used a hidden dependency to fetch a second-stage payload and erase traces after installation.