cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Japan's Digital Agency, which operates the Government Solution Service used by multiple ministries, has confirmed a data breach after attackers exploited a vulnerability in a VPN appliance. Approximately 246,000 records were exposed, including names and contact details belonging to government officials and contractors, while financial information was not affected.
- Two oil tankers bound for Texas were hit by cyberattacks that disrupted onboard systems during voyages to the United States. US Coast Guard and FBI personnel boarded the vessels, while officials confirmed malicious cyber activity on the VL Prosperity but have not publicly attributed the attacks to a specific actor.
- Brevo, a French customer communication and marketing platform, has confirmed a supply chain attack after attackers used a compromised Cloudflare API key to inject malicious ClickFix scripts into websites that use Brevo components. The attack affected about 100,000 websites.
- Japanese software company Helpfeel, operator of image-sharing service Gyazo, has reported a data breach after attackers exploited a vulnerability in an image upload server. Above 23 million user records and 490 million image metadata records were exposed, including email addresses, password hashes, session IDs, integration tokens, and location metadata.

AI THREATS

- Check Point Research has analyzed the July-August AI threat landscape, highlighting the latest cases when AI models broke out of their evaluation environments. On the attackers' side, AI is increasingly used as an operational tool, while the AI systems themselves are also targeted. The report highlights AI-assisted ransomware intrusions, criminal markets for stolen model access, and vulnerabilities in coding agents and enterprise copilots.
- Researchers uncovered Luciferus, an uncensored AI service advertised on an underground forum for malware creation and other prohibited activities. Testing showed that the service could generate code for a simple remote access trojan, while its operator markets several paid tiers to users seeking unrestricted AI assistance.
- Researchers unveiled BragJack, an attack that allows malicious browser extensions to hijack AI assistants by forcing prompts through trusted browser channels. The technique affected several AI-enabled browsers and assistants, enabling actions such as file access, screenshots, microphone and camera use, and logged-in activity before vendors issued security fixes.

VULNERABILITIES AND PATCHES

- Check Point has released a fix for CVE-2026-91843, a critical vulnerability affecting Security Management and Log Servers. The flaw, rated CVSS 9.8, stems from a stack overflow in the login process and can allow unauthenticated remote attackers to execute code as root on affected R80 through R82 systems.
- Cisco has addressed CVE-2026-76460 & CVE-2026-76461, two critical vulnerabilities affecting Cisco ISE and Secure Email Gateway with CVSS scores of 10.0 and 9.8. According to Cisco, the company is aware of active exploitation of CVE-2026-76460, which allows an unauthenticated remote attacker to gain access to the system's management interface.
- Oracle has released its September 2026 Critical Security Patch Update, addressing more than 800 vulnerabilities across 17 product families. More than 100 flaws are rated critical, while over 240 can be exploited remotely without authentication. Affected products include E-Business Suite, Fusion Middleware, Hyperion, Siebel CRM, Analytics, Communications, and Virtualization.
- ISC has published security updates for BIND 9 addressing 14 vulnerabilities, including seven high-severity flaws that can trigger denial-of-service conditions. One issue, CVE-2026-77692, allows an unauthenticated remote attacker to crash the named process with a single crafted DNS-over-HTTPS request. Versions 9.21.26 and 9.20.29 contain the fixes

THREAT INTELLIGENCE REPORTS

- US, Japanese, Australian, and German authorities warned about WaterPlum (Contagious Interview), a North Korea-linked campaign that infected at least 30,000 devices across more than 100 countries. Operators posed as AI or blockchain employers, targeting IT professionals and stealing funds or credentials from over 7,000 cryptocurrency wallets from December 2025 through July 2026.
- Researchers outlined a China-aligned FamousSparrow espionage campaign targeting government entities across Latin America and a telecommunications organization in Puerto Rico. The group deployed a new backdoor called SparroWocky, replacing its long-running SparrowDoor implant and supporting persistent surveillance across victims in Latin America.
- Researchers revealed HEAVYGRAM, a Windows surveillance backdoor linked with moderate confidence to the Iranian Handala group. Active since 2023 against Iranian dissidents and journalists, the malware uses Telegram for command and control and can execute commands, capture screenshots, steal Telegram session data, exfiltrate files, and maintain persistence.
- Researchers identified GhostCode, a device-code phishing kit that targets Microsoft 365 accounts by abusing the legitimate OAuth 2.0 device authorization flow. Victims authenticate through Microsoft, allowing attackers to capture tokens, register attacker-controlled devices, and obtain persistent account access without stealing the victim's password or directly bypassing MFA.