CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Latvia's Road Traffic Safety Directorate (CSDD) has confirmed a breach affecting payment records of more than 1.2 million people - roughly two-thirds of the country's population - as well as 200,000 organizations. The stolen data included identification numbers, license plates, payment amounts, dates and addresses. Attackers reportedly exploited a vulnerability in an internet-facing system.
- Sakura Internet, a Japanese cloud and hosting provider, has disclosed unauthorized access involving rental server environments and a separate sales management system. Up to 1.36 million customer accounts may have been exposed. Attackers also accessed hundreds of rental server accounts and installed malware on affected environments.
- The Hospital for Sick Children, Canada's largest pediatric hospital, has disclosed data theft involving a third-party application. The incident affected its careers website and exposed information belonging to employees, applicants and staff at related organizations. The hospital stated that clinical systems and patient information were not affected.
- Berlin authorities isolated the city's urban development and mobility ministries from government IT networks following a security breach. The measure disrupted email and internet access, forcing employees to use alternative communication channels and delaying several public services while the ministries remained disconnected.

AI THREATS

- Researchers have demonstrated an autonomous AI agent exploiting a GitHub Actions flaw in Snowflake's public repository, gaining read access to the company's internal Jira system. The agent exfiltrated tokens within seconds. Snowflake patched the workflow and rotated credentials after the demonstration, which required no human steering.
- US authorities warn of active AI-assisted attacks targeting Siemens S7 industrial controllers across manufacturing, energy, water and other critical sectors. Attackers use AI-generated scripts disguised as monitoring tools and open-source libraries to probe internet-exposed attempting to cause unauthorized configuration changes, operational disruption or damage to industrial equipment.
- Researchers have analyzed 'Kriminal', a publicly accessible AI platform marketed as uncensored and offering social engineering and exploit assistance through cryptocurrency subscriptions. The service combines models including Grok, Claude and Llama, allowing users to generate phishing content, malicious code and other cybercrime material while reducing reliance on a single provider.

VULNERABILITIES AND PATCHES

- GitLab has released out-of-band fixes for CVE-2026-19478, a critical unauthenticated code injection vulnerability affecting self-managed Community and Enterprise editions. Rated CVSS 9.4, the flaw can let remote attackers alter or delete public projects and user data. Exploitation attempts were observed after disclosure.
- Cisco has released fixes for nine critical vulnerabilities affecting Crosswork platforms and Secure Workload software, including six flaws rated CVSS 10.0. The issues include authentication, access-control and file-system weaknesses that could enable unauthorized access or system compromise.
- Citrix has published patches for CVE-2026-19489 and CVE-2026-19490 affecting NetScaler ADC and NetScaler Gateway. The critical authentication bypass flaw can let unauthenticated attackers access appliances configured with SAML authentication, while the second vulnerability can cause denial of service.
- NASA/JPL has fixed a critical vulnerability in the open-source AMMOS Instrument Toolkit AIT-GUI that enables unauthenticated command execution through its web console. Rated CVSS 9.4, the flaw can allow remote command execution, script launches and sequence execution. AIT-GUI version 2.5.2 contains the fix.

THREAT INTELLIGENCE REPORTS

- Check Point Research has investigated StopAndProtect campaign which abuses thousands of compromised WordPress sites to distribute malware and store stolen data. The campaign combines ransomware with data theft and uses ClickFix technique to infect visitors. Operational mistakes exposed logs, screenshots and victim IP addresses.
- Check Point Research has investigated the Windows Defender Boot-Time Removal driver, BTR.sys, showing that the Microsoft-signed remediation component can be repurposed to perform privileged file and registry changes during startup. Researchers developed BTR_CLI to craft encrypted tasks and found that multiple versions share a hard-coded RC4 key.
- Check Point Research have uncovered increased targeting of the education sector ahead of the school year. Organizations averaged 4,696 weekly attacks from January through July 2026, increase of 8%. Attackers also registered education-themed domains and used seasonal phishing lures impersonating schools and student reward programs to steal credentials.
- Researchers have tracked a Cl0p extortion campaign exploiting CVE-2026-12569 in PTC Windchill and FlexPLM, with more than 40 organizations named by the group. Analysis identified a custom implant capable of decrypting credentials, accessing databases and supporting bulk data theft from compromised product lifecycle management environments.

  Check Point IPS provides protection against this threat *(PTC Multiple Products Remote Code Execution (CVE-2026-12569))*