Weekly Cybersecurity Briefing (14 September – 20 September 2026)

CyberSecBrief Team

CyberSecBrief provides clear, concise cybersecurity briefings that summarise the most relevant developments of the week. The report highlights notable incidents, key themes, and significant activity across the threat landscape, supported by daily updates sourced from trusted feeds and advisories. Its purpose is to offer a practical, time-efficient overview for readers who need a reliable snapshot of current cybersecurity events.
For more briefings, visit CYBERSECBRIEF.COM.

September 21, 2026

Editorial Analysis

AI agents appeared repeatedly across this week's reports, in both offensive activity and as targets themselves. Spain's **AEPD** documented an incident involving an autonomous AI agent that logged into a real organisation, scanned for vulnerabilities and modified data. **Hacktron** used Claude Opus 5 in authorised research to chain a libheif flaw with an SSO misconfiguration into OpenAI account takeover. **BragJack** took the other side of the equation, hijacking browser-embedded AI assistants by manipulating the network requests used to retrieve their instructions across five major browsers. The incidents cover different attack paths, but all involve agents operating with access that can extend well beyond the model itself.

Malicious code also continued moving deeper into software and service infrastructure. **GHAPPIER** and **indexed-btree** placed their payloads in runtime code rather than npm installation scripts, while **KREMLIN** and PolinRider-linked campaigns used Ethereum smart contracts for command and control. Brevo's compromised Cloudflare account was used to distribute malware across more than 100,000 sites, and CrowdSec traced a separate exposure to an ex-employee's retained access following an earlier supply-chain compromise. These incidents show how much of an operation can now sit inside legitimate development, hosting and service infrastructure, making the initial compromise only one part of the attack path.

Cisco also disclosed its third maximum-severity, actively exploited vulnerability in as many weeks. **CVE-2026-76460**, affecting Identity Services Engine, follows recent critical issues in Secure Email Gateway and other Cisco enterprise platforms. The frequency is notable, although this week's evidence does not establish whether it reflects greater scrutiny of Cisco's code or sustained targeting of its products.

Highlights of the Week

BragJack Hijacks AI Assistants Built Into Five Major Browsers

Security researchers found flaws in AI agents built into Chrome, Edge, Opera Neon, Perplexity Comet and Claude in Chrome. A malicious browser extension manipulated network requests to redirect trusted domains controlling each agent, using a technique called Prompt Forcing to bypass prompt injection defences. The zero-click attacks enabled file access, camera and microphone activation, and email exfiltration, earning over $20,000 in bounties.

Sources:

- Forever Security

Cisco Discloses Third Maximum-Severity Flaw in Three Weeks

Cisco disclosed CVE-2026-76460, a CVSS 10.0 authentication bypass in Identity Services Engine, already under active exploitation, following critical flaws in Secure Email Gateway and Nexus Dashboard earlier in the week. ISE sits at the centre of network identity and policy, so a successful bypass grants root-level access to a system controlling device and user authorisation across affected networks.

Sources:

- Cisco
- Cisco

North Korean WaterPlum Group Confirmed to Have Infected 30,000 Devices

Coordinated reporting from Japan, the US, Australia and Germany confirmed North Korea's WaterPlum group, also known as Contagious Interview, has infected over 30,000 devices and stolen roughly $10.71 million from more than 7,000 cryptocurrency wallets. The group poses as recruiters, tricking developers into running malicious npm packages containing malware such as BeaverTail and InvisibleFerret during fake job interviews.

Sources:

- FBI Internet Crime Complaint Center

Spain Reports First Data Breach Attributed to an AI Agent

Spain's data protection authority, AEPD, received its first notification of a personal data breach reportedly executed autonomously by an AI agent. The agent logged into a target system, searched for vulnerabilities, modified personal data and accessed invoices, though AEPD cautioned this does not confirm the underlying AI provider's infrastructure was compromised.

Sources:

- Agencia Española de Protección de Datos

Researchers Chain Flaws to Hijack OpenAI Employee Accounts Using Claude

Hacktron researchers combined a years-old libheif memory-safety flaw with an OpenAI SSO misconfiguration to take over employee ChatGPT and Codex accounts, eventually reaching an internal code repository. The chain began with a compromised forum account and used Anthropic's Claude Opus 5 to help execute the multi-step exploit, which OpenAI and Discourse have since patched.

Sources:

- Hacktron

Threats

Iranian Spyware CHOSEN BRICK Targets Dissidents With Fake MRI Scans

British, American and Dutch agencies exposed CHOSEN BRICK, Iranian state-sponsored spyware delivered via social engineering lures including fake MRI scans. The Windows-only malware harvests contacts, messages and screen content, activates microphones, and communicates through individual Telegram bots per victim.

Sources:

- National Cyber Security Centre

China-Linked FamousSparrow Deploys New SparroWocky Backdoor

ESET identified SparroWocky, a modular C++ backdoor deployed by China-aligned group FamousSparrow since August 2025, replacing its previous SparrowDoor implant. The malware targets governmental organisations across Latin America and incorporates anti-analysis techniques including call-stack spoofing.

Sources:

- ESET (WeLiveSecurity)

Infrastructure & Exploits

Critical GitLab Path Traversal Flaw Actively Exploited

GitLab disclosed CVE-2026-85706, a maximum-severity path traversal flaw in the repository commits API allowing unauthenticated attackers to read arbitrary server files. CISA added the flaw to its Known Exploited Vulnerabilities catalog with a federal remediation deadline of 14 September 2026.

Sources:

- Orca Security
- Rapid7

Check Point Discloses Critical Server Hijack Flaw

Check Point disclosed CVE-2026-91843, a critical vulnerability scoring 9.8 on CVSS affecting its Security Management and Log Servers. The flaw could let an unauthenticated attacker remotely execute arbitrary code with root privileges via the login process, with a LivePatch fix now available.

Sources:

- Check Point

Tools & Techniques

NPM Supply Chain Attacks Shift Malware Into Runtime Code

GHAPPIER and the indexed-btree malware family moved malicious logic away from npm install scripts and into code that only executes when a package is used. GHAPPIER carried valid provenance through GitHub's trusted-publishing pipeline, while indexed-btree hid its loader inside a commonly called prototype method and used an Ethereum smart contract for command and control.

Sources:

- CloudSEK
- Checkmarx

CrowdSec Source Code Leaked Following TanStack Supply Chain Compromise

An attacker published CrowdSec's private GitHub source code on a hacking forum, traced to a former employee compromised via the May TanStack npm supply chain attack. The threat actor used a since-expired OAuth token to clone over 170 private repositories, though CrowdSec's infrastructure and databases remained unaffected.

Sources:

- CrowdSec

Brevo Supply Chain Attack Hits Over 100,000 Sites

Email marketing provider Brevo served malware to visitors of its own site and more than 100,000 customer sites after attackers breached its Cloudflare account. The injected script installed a backdoored WordPress plugin for admins or showed other visitors a Clickfix overlay tricking them into running malicious commands.

Sources:

- Sansec

Policy & Legal

FBI Seizes Domains Behind Long-Running NightmareStresser DDoS Service

The FBI, working with the Royal Canadian Mounted Police, seized domains linked to NightmareStresser, a DDoS-for-hire service that launched hundreds of thousands of attacks since

2022. The action forms part of Operation PowerOFF, an ongoing international effort targeting DDoS-for-hire infrastructure.

Sources:

- US Department of Justice

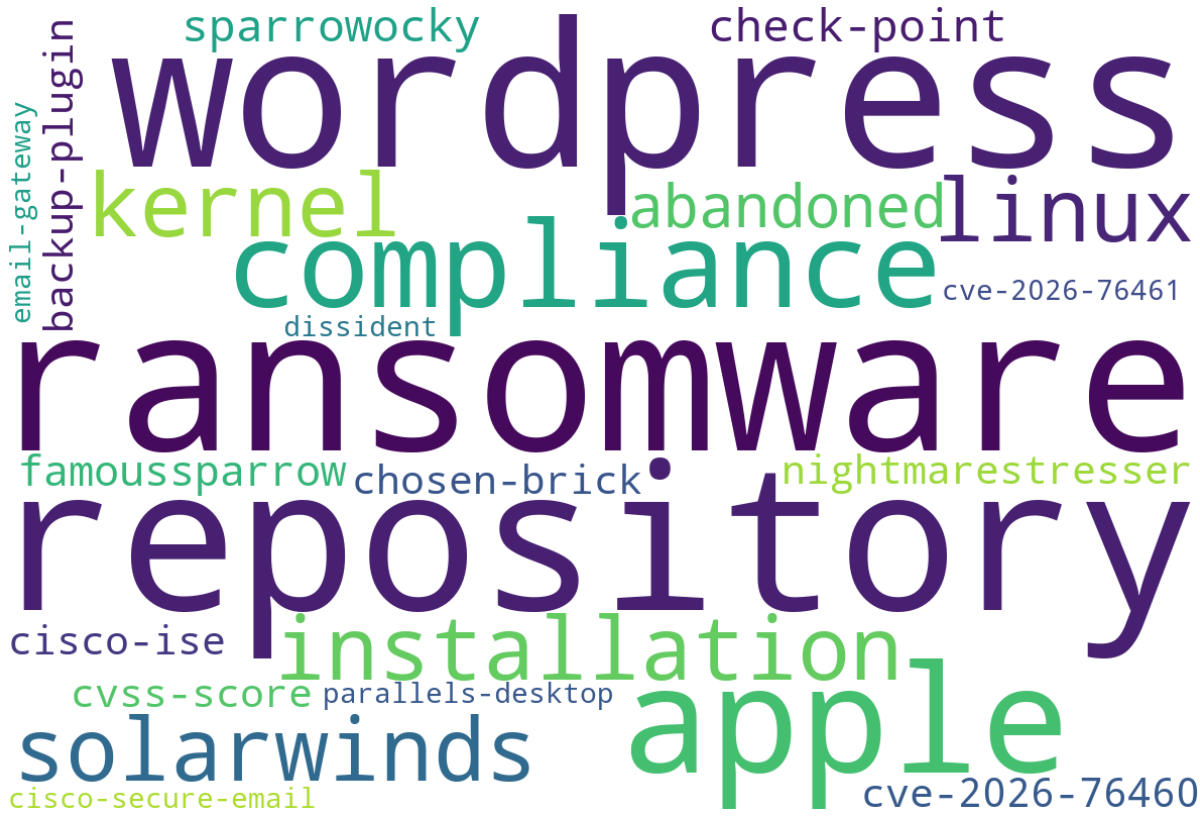
CISA Issues Guidance on Cyber Decoys for Threat Detection

CISA published guidance helping defensive teams plan and deploy cyber decoy strategies, addressing tripwires, breadcrumbs and honeytokens using MITRE Engage and MITRE ATT&CK frameworks. The guidance targets organisations adopting Zero Trust models across varying levels of cybersecurity maturity.

Sources:

- CISA

Weekly Topic Distribution



Copyright and Legal Notice

Disclaimer & Terms of Use

CyberSecBrief is a personal, non-commercial project operated from Germany and is not affiliated with any company or organisation. The information provided is intended solely for general informational and educational purposes and does not constitute professional cybersecurity, legal, or financial advice. Security-related information changes rapidly; although accuracy and timeliness are sought, no guarantee is given regarding completeness, correctness, or applicability. Users must verify details with official sources or qualified professionals before making decisions.

The owner disclaims liability for any indirect, incidental, or consequential damages arising from reliance on this material. External links and third-party feeds are offered for convenience; their content, accuracy, availability, and privacy practices are outside our control and are not endorsed. Sponsored or promoted material may appear, yet inclusion does not imply endorsement.

Original content is protected by copyright. Where external material is used, appropriate attribution is provided. Reproduction of original content without prior written consent is prohibited. Content may be updated, modified, or removed at any time without notice.

This disclaimer and the Terms of Use are governed by the laws of Germany and applicable European Union regulations. Should any provision be deemed invalid, the remaining provisions shall continue in full force and effect.

Credits and Sources

CVE entries are sourced from the CVE® Program, operated by The MITRE Corporation, and from the National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology (NIST). The NVD is provided “as is” without warranty of any kind.

Definitions for APT groups are derived from the MITRE ATT&CK® knowledge base, reproduced and distributed with the permission of The MITRE Corporation. © 2025 The MITRE Corporation.

All feeds and advisories are properly acknowledged and linked to their original sources where referenced, including within briefings.

Logo icon created by Ida Desi Mariana — Flaticon.

Powered by CyberFeedBites.

Source

This briefing is published by *CyberSecBrief* –
https://www.cybersecbrief.com/