CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Manchester Airports Group, the UK operator of Manchester, London Stansted, and East Midlands airports, has disclosed a cyberattack that exposed data belonging to about 8.7 million customers. The compromised information includes contact details, vehicle registration numbers, and information collected through car park, lounge, fast-track, and Wi-Fi registrations.
- The U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives has confirmed a cyberattack affecting a standalone computer containing information on ATF investigation targets. The system was disconnected after the compromise, while the Qilin ransomware group listed the agency on its leak site and claimed responsibility.
- Boston Scientific, a US-based global medical device company, has experienced a cyberattack that caused network outages and disrupted operations worldwide. Access to internal systems and applications, including services supporting order processing and shipping, was affected. The company began restoring impacted systems following the August 26 disruption.
- McKesson, a major U.S. healthcare and pharmaceutical company, has disclosed a data breach involving unauthorized access to third-party applications and data theft. Threat group ShinyHunters claimed it used vishing to compromise Okta accounts and access Salesforce and Snowflake, exfiltrating about 1TB of data containing approximately 284 million patient-related records.

AI THREATS

- Researchers described Cryptographic Context Injection, a technique that conceals malicious instructions inside encrypted content to bypass safeguards in AI assistants with browsing and code capabilities. During testing, Grok was induced to expose user conversation data while Gemini generated content that would normally be blocked by its safety controls.
- Researchers detailed a prompt injection vulnerability in Amazon Kiro, an AI development environment, that could allow malicious workspace files to manipulate the agent and transmit local information. Exploitation required a user to open a crafted project and interact with Kiro. Amazon addressed the issue in version 0.8.140.
- Researchers profiled AnonyMousKIT, an AI-enabled phishing-as-a-service operation targeting owners of stolen iPhones. The platform uses email, text messages, WhatsApp, and AI-generated voice calls to steal Apple IDs, passcodes, and two-factor authentication codes, helping criminals remove Activation Lock and gain access to associated accounts.

VULNERABILITIES AND PATCHES

- PaperCut released emergency fixes for two actively exploited vulnerabilities affecting PaperCut NG and MF. CVE-2026-81578, rated CVSS 8.8, enables authentication bypass, while CVE-2026-82078, rated CVSS 9.4, involves unsafe class loading. Attackers can chain the vulnerabilities to achieve unauthenticated remote code execution on affected servers.
- Ubiquiti patched 21 critical and high-severity vulnerabilities affecting UniFi Protect, Network, Access, Talk, UniFi OS, and other products. The flaws include authentication bypass, command injection, and privilege escalation issues, with several receiving CVSS scores of 10.0. Successful exploitation could allow attackers to gain administrative control over affected devices.
- Vercel addressed two critical vulnerabilities affecting Next.js, including CVE-2026-75604, a Windows-specific path traversal flaw, and a libheif AVIF image-processing vulnerability. Both can result in unauthenticated remote code execution under affected configurations. Fixes are included in Next.js versions 15.5.24 and 16.3.3. A public proof-of-concept is available for the AVIF issue.
- ServiceNow has addressed three critical vulnerabilities in its AI Platform, CVE-2026-18885, CVE-2026-18886, and CVE-2026-74820, all rated CVSS 10.0. The flaws involve code injection, access control, and SQL injection and can allow unauthenticated attackers to execute code, escalate privileges, or access and modify instance data.

THREAT INTELLIGENCE REPORTS

- Check Point researchers identified a large-scale phishing campaign using fraudulent debt-relief emails to manipulate victims into calling attacker-controlled phone numbers. The campaign targeted more than 9,000 organizations and distributed approximately 24,700 emails within 14 days. Phone conversations were then used to obtain victims' personal and financial information.
- U.S. authorities announced the disruption of QScan and QTRouter, two platforms operated by China-linked group QTFY to target U.S. critical infrastructure and government networks. QScan infected internet-connected devices, while QTRouter used compromised systems to conceal the origin of intrusion activity targeting agencies including NASA, the Federal Reserve, and Department of Energy.
- Researchers unveiled an expanded toolset used by the Iran-linked Nimbus Manticore threat group to target organizations in the Middle East and Europe. The campaign includes an SSH tunneling utility and a C++ backdoor resembling TWOSTROKE, providing attackers with persistent remote access and command execution on compromised systems.
- Researchers discovered a Chinese threat actor exploiting known ownCloud and WordPress vulnerabilities to compromise sensitive organizations in the Philippines. Victims included a nuclear research agency and a marine engineering contractor supporting the Philippine Navy. The attackers obtained reactor-related records, employee information and credentials, among other data.