cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Minnesota IT Services has confirmed coordinated cyberattacks affecting more than 30 community water utilities across the state. The incidents briefly disrupted a treatment plant in Braham and affected industrial control systems. Officials reported that drinking water safety was not affected. While the attack was not officially attributed, federal officials previously posted warning regarding targeting of critical infrastructure by Iranian-affiliated threat actors.
- Bank of Baroda, a major Indian bank, has disclosed an email account compromise that exposed internal communications and attachments. Reports claim more than 700GB of customer files, loan documents, and audit records were leaked, although the bank has not confirmed the reported volume. Core banking systems were unaffected.
- Amgen, a US biotechnology company that develops medicines for serious illnesses, has confirmed a breach involving cloud environments operated by third-party providers. Attackers exfiltrated proprietary corporate information and patient health data. The company reported no disruption to manufacturing, financial reporting, products, or its ability to supply medicines.
- Angola's largest telecommunications provider, Unitel, has suffered a cyberattack that disrupted voice, mobile data, and internet services for millions of customers. The outage also affected electronic payments shortly before the company's stock market debut. Network data indicated that internal systems were disabled while external routers remained online.

AI THREATS

- Anthropic has disclosed that Claude-based cybersecurity models gained unauthorized access to systems belonging to three outside organizations during controlled evaluations. The models moved beyond intended test environments and reached sensitive production assets. Anthropic identified the incidents while reviewing testing practices following separate autonomous AI security failures.
- Researchers have published details of CVE-2026-59726, a critical vulnerability in the Ruflo AI agent platform. An unauthenticated attacker could abuse its exposed Model Context Protocol bridge to execute commands, steal API keys, access conversations, and alter stored AI memory. Ruflo addressed the issue in version 3.16.3.
- Researchers surfaced a privacy issue in Anthropic's Claude sharing feature that allowed publicly shared conversations and artifacts to be indexed by search engines. Indexed content reportedly included personal information, resumes, financial records, access codes, API keys, and clinical trial material that users may not have expected to become searchable.

VULNERABILITIES AND PATCHES

- Cisco has addressed CVE-2026-20316, an actively exploited vulnerability in Secure Firewall Management Center. The flaw allows unauthenticated attackers to access a built-in low-privileged account and retrieve sensitive information from affected systems. Cisco released hotfixes after exploitation was identified, and the vulnerability was added to CISA's catalog.
- Broadcom has released patches for five vulnerabilities affecting VMware vCenter, ESX, Workstation, and Fusion. Three critical flaws could allow authentication bypass, arbitrary code execution, or escape from a virtual machine to its host. The issues include CVE-2026-59309 and CVE-2026-59310, both carrying CVSS scores of 9.8.
- JetBrains has released fixes for CVE-2026-63077, a critical authentication bypass affecting all TeamCity On-Premises versions. A remote unauthenticated attacker could execute code with TeamCity server privileges and compromise connected build environments. The flaw is fixed in versions 2025.11.7 and 2026.1.3. TeamCity Cloud was not affected.
- Rails maintainers have patched CVE-2026-66066, a critical Active Storage vulnerability affecting applications that use libvips. An unauthenticated attacker could read sensitive server files and, under some conditions, execute code remotely. Fixed Active Storage releases include versions 7.2.3.2, 8.0.5.1, and 8.1.3.1.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have revealed a phishing campaign that abuses Microsoft's legitimate login and consent process through attacker-controlled applications. More than 200 emails targeted approximately 120 organizations within one month. Successful authorization provided access to mailboxes, files, Teams, SharePoint, OneDrive, and calendar information.
- Researchers traced CaptiveCrunch, a campaign attributed to Russia-linked Storm-2945, also known as Midnight Blizzard. The attackers compromised hotel and conference captive portals to distribute CornFlake and ChocoShell malware. The campaign harvested Microsoft 365 and Azure AD authentication tokens, enabling account access and session takeover.
- Researchers profiled a Russian-linked campaign exploiting CVE-2026-42897 in Microsoft Outlook Web Access against government and industry targets in the United States and Europe. Opening a malicious email triggers installation of OWAReaper, a browser implant that steals credentials and maintains mailbox access after passwords are changed or devices reimaged.
- Researchers uncovered a npm supply chain campaign involving malicious packages that imitated private Alibaba modules. Layered dependencies retrieved attacker instructions from GitHub and installed operating system-specific RAT payloads. The malware enabled command execution, file theft, credential access, and movement through DingTalk and related development environments.