



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

14 September 2026

Vulnerabilities

NCSC Warns of Critical Check Point VPN Flaws as Large-Scale Exploitation Is Expected

Cyber Security News - 14 September 2026 06:11

The Dutch National Cyber Security Center (NCSC) has issued an urgent warning over two critical vulnerabilities in Check Point VPN products, saying it expects large-scale exploitation attempts in the near term. Organizations using affected Check Point gateways, management systems, or Spark Firewall products should deploy the available fixes immediately.

Critical Dell ObjectScale Vulnerabilities Allows Malicious Users to Compromise the Affected system

Cyber Security News - 13 September 2026 15:43

Dell Technologies released a security advisory about multiple vulnerabilities affecting Dell ObjectScale and Elastic Cloud Storage (ECS) deployments. Including a critical remote code execution flaw that could let an unauthenticated attacker compromise vulnerable systems. The advisory, tracked as DSA-2026-393, was published on September 10, 2026.

Multiple VLC Media Player Vulnerabilities Allow Attackers to Corrupt or Read Heap Memory

Cyber Security News - 12 September 2026 15:31

Two security vulnerabilities in VLC Media Player could allow attackers to corrupt heap memory or disclose sensitive data from a victim's memory. The flaws, tracked as CVE-2026-56711 and CVE-2026-73324, affect VLC Media Player versions 3.0.0 through 3.0.23 and require a victim to open a specially crafted media file or playlist entry.

CISA: Hackers now exploit max severity GitLab flaw in attacks

BleepingComputer - 14 September 2026 04:06

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned that hackers are now exploiting a maximum-severity GitLab vulnerability in attacks. [...]

Attackers Exploit Critical Cisco FMC Flaw to deploy Qilin ransomware

Security Affairs - 11 September 2026 11:14

Three threat groups are exploiting two Cisco FMC flaws to steal credentials, gain root access and deploy Qilin ransomware. Cisco Talos says three separate threat groups are exploiting two recently patched Secure Firewall Management Center (FMC) flaws.

Attackers Chain JFrog Artifactory Flaws to Gain Admin Control and Plant Backdoors

The Hacker News - 11 September 2026 14:01

Attackers have chained two flaws in JFrog Artifactory, the repository that software build pipelines pull from, to take administrator control of self-hosted servers and plant backdoors, cloud security company Wiz said in a report.

Threat actors and malware

Hackers Abuse Autolt to Inject AsyncRAT Into Microsoft-Signed Windows Process

Cyber Security News - 14 September 2026 08:07

Hackers are using a familiar Windows automation tool to hide AsyncRAT, a remote-access trojan, inside a trusted system process.

Researchers say OpenAI agents were behind May hacking campaign targeting RubyGems

CyberScoop - 12 September 2026 02:50

OpenAI confirmed their agents were behind a campaign in May that researchers say flooded the popular online code repository with malicious software packages.

Hackers exploit Tencent app flaw to deploy GrayRabbit malware

BleepingComputer - 13 September 2026 11:26

Threat actors linked to a China-aligned espionage group are exploiting a critical vulnerability (CVE-2026-51990) in Tencent's Sogou Input Method for Windows to deploy the GrayRabbit backdoor. [...]

Hackers abused Claude to extract secrets from 1.8M Android apps

BleepingComputer - 11 September 2026 17:19

Anthropic says multiple threat groups, including the financially motivated and state-sponsored espionage groups linked to Russia and China, tried to abuse its Claude AI model for malicious purposes. [...]

Artifactory flaws chained in attacks deploying backdoor malware

BleepingComputer - 11 September 2026 13:29

Threat actors are exploiting critical and high-severity vulnerabilities in JFrog Artifactory to bypass authentication, gain administrative privileges, and deploy a Rust backdoor on vulnerable self-hosted servers. [...]

Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data

The Hacker News - 13 September 2026 16:41

Microsoft has disclosed details of two campaigns in which threat actors are abusing third-party email delivery infrastructure to blast financial fraud scam messages and using passkey-



Scottish
Cyber
Coordination
Centre

themed social engineering to breach cloud environments. The first campaign, per the tech giant, involved sending over a million scam emails between August 3 and 5, 2026, by masquerading as chief executive officers

Papercut AI Swarm Attack Heralds Changes for Cyber Kill Chain

darkreading - 11 September 2026 16:48

From creating lab environments for staging and testing agentic attacks to reconnaissance to lateral movement and exfiltration, the most innovative attackers are widely incorporating AI.