



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

18 September 2026

Vulnerabilities

[U.S. CISA adds Acronis Backup, Cisco ISE, and Google Pixel flaws to its Known Exploited Vulnerabilities catalog](#)

Security Affairs - 17 September 2026 10:26

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Acronis Backup, Cisco ISE, and Google Pixel flaws to its Known Exploited Vulnerabilities catalog.

[Cisco Warns of New Zero-Day ISE Auth Bypass \(CVSS 10.0\) Exploited in Active Attacks](#)

The Hacker News - 17 September 2026 13:09

Cisco has warned of a fresh maximum-severity security flaw impacting Identity Services Engine (ISE) that has come under active exploitation. The vulnerability, tracked as CVE-2026-76460 (CVSS score: 10.0), could allow an unauthenticated, remote attacker to bypass authentication.

[Critical Docker Sandboxes Flaw Lets Malicious Guest Code Read and Modify macOS Host Files](#)

The Hacker News - 17 September 2026 22:07

Malicious code running inside a Docker Sandboxes virtual machine on macOS could escape the project directory shared into it and read or change files anywhere else on the host, Docker warns in a security announcement on September 15.

[Critical Check Point Management Flaw Lets Unauthenticated Attackers Run Code as Root](#)

The Hacker News - 18 September 2026 00:38

A critical vulnerability in Check Point's Security Management and Log Servers could allow an attacker without login credentials to run code as root on those servers over the network. The Security Management Server is the system that controls firewall policy and administrator access.

[Critical Unbound DNSSEC Validator Flaw Could Allow RCE via a Malicious DNS Zone](#)

The Hacker News - 17 September 2026 19:00

Every release of the Unbound DNS resolver before 1.26.1 has a critical heap overflow in its DNSSEC validator, maintainer NLnet Labs said in an advisory on Wednesday. An attacker who controls a malicious zone and queries a vulnerable resolver can trigger it, enabling remote code execution.



Scottish
Cyber
Coordination
Centre

CISA Ditches Weekly Vulnerability Roundups for Risk-Based Focus

darkreading - 17 September 2026 22:23

The move is consistent with the agency's advice on the need for organizations to prioritize the vulnerabilities that actually matter.

Threat actors and malware

New RatHat Android malware uses AI to automate device control

BleepingComputer - 17 September 2026 18:50

A new Android malware called RatHat has been discovered, targeting users with an AI-powered subsystem that helps operators remotely navigate compromised devices.

Brevo supply-chain attack injected ClickFix scripts on customer sites

BleepingComputer - 17 September 2026 14:11

Brevo confirmed that attackers stole a Cloudflare API key and used it to inject malicious ClickFix scripts into its websites and JavaScript files embedded on customer sites to distribute malware.

SilkParasite Infrastructure Links SpiceRAT to Central Asian Targets

Security Affairs - 17 September 2026 15:16

Hunt.io and researcher Guy Yasur have traced a tight cluster of SpiceRAT command-and-control servers that predate and extend Bitdefender's August 2026 SilkParasite report.

U.S. Seizes NightmareStresser Domains Linked to Hundreds of Thousands of DDoS Attacks

The Hacker News - 17 September 2026 11:43

The U.S. Department of Justice (DoJ) on Tuesday announced the court-authorized seizure of internet domains associated with a distributed denial-of-service (DDoS)-for-hire service known as NightmareStresser.