



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

19 October 2026

Vulnerabilities

[Google Fixes 10 Chrome Vulnerabilities, Including Memory Corruption Flaw Found With Claude AI](#)

Cyber Security News - 17 October 2026 06:29

Google released a Chrome Stable security update fixing 10 vulnerabilities across Windows, Mac, and Linux, including a high-severity DOM memory corruption flaw reported by Xinyang Ge of Anthropic with Claude AI. The update also addresses one critical, six high-severity, and three medium-severity vulnerabilities.

[Hackers Exploit Critical Collabora Online Flaw to Backdoor Nextcloud Servers](#)

Cyber Security News - 17 October 2026 06:24

Hackers are exploiting a critical flaw in the Collabora Online Built-in CODE Server app for Nextcloud, with users reporting web shells on compromised servers. Tracked as CVE-2026-110447, the vulnerability allows remote attackers to run operating system commands without logging in.

[CC-4870 - Active Exploitation of BeyondTrust Remote Support Vulnerability \(CVE-2026-102764\)](#)

NHS Digital - 16 October 2026 12:07

Severity: High Successful exploitation of CVE-2026-102764 could allow a remote, unauthenticated attacker to upload arbitrary files on affected appliances Successful exploitation of CVE-2026-102764 could allow a remote, unauthenticated attacker to upload arbitrary files on affected appliances Updated: 16 Oct 2026

[Hackers exploit SiteGuard WAF flaw to run commands as admins](#)

BleepingComputer - 18 October 2026 11:23

Attackers are targeting an OS command injection vulnerability in SiteGuard Server Edition that lets them execute commands as root or SYSTEM on affected servers. [...]

[Drupal patches critical RCE flaws, warns exploits may emerge soon](#)

BleepingComputer - 17 October 2026 11:32

Drupal has patched two critical vulnerabilities that could allow attackers to execute code remotely on websites running any supported version of the content management system. [...]

[Critical BlockStrap flaw lets hackers run code on Magento servers](#)

BleepingComputer - 16 October 2026 17:00



Scottish
Cyber
Coordination
Centre

Researchers warn that hackers could soon exploit a maximum-severity vulnerability (CVE-2026-103849) affecting Magento and Adobe Commerce, potentially allowing them to execute arbitrary PHP code on store servers. [...]

Unpatched Broadcom Wi-Fi Flaw Lets Attackers in Range Run Code as Root on Routers

The Hacker News - 19 October 2026 12:59

A flaw in Broadcom's Wi-Fi setup software lets an attacker within radio range run code as root on Broadcom-based routers, without the network password or any pairing step, security researcher Quentin Kaiser disclosed on October 16.

F5, Juniper Networks Patch Critical Vulnerabilities

SecurityWeek - 16 October 2026 10:54

Successful exploitation of some of these issues could lead to remote code execution and full device takeover.

Microsoft Patches Two Dozen RCE Flaws in Office

SecurityWeek - 16 October 2026 08:55

In addition to RCE flaws, Microsoft fixed multiple information disclosure bugs and a security bypass issue in Office.

Threat actors and malware

Hackers used Compromised ConnectWise Backup Credentials to Hack 173 Microsoft 365 Accounts

Cyber Security News - 17 October 2026 11:52

Hackers used a stolen ConnectWise Cloud Backup credential to sign in to 173 Microsoft 365 partner and customer tenants, giving them access through a trusted backup application. The incident shows how one leaked vendor secret can create risk across many organizations when a multitenant app already has wide permissions.

Hackers Use New ROMULUS ClickFix Platform to Deliver Malware and Evade Security Detection

Cyber Security News - 16 October 2026 15:42

Hackers are using a newly identified platform called ROMULUS to deliver malware through ClickFix traps, combining hidden PowerShell scripts, altered software installers, and encrypted archives. The platform supports separate infection paths, including one that installs LegionLoader and another that abuses a legitimate Stardock program to load malicious code. The findings show how a single delivery [...]

Hackers breach Microsoft 365 tenants via ConnectWise supply-chain attack

BleepingComputer - 17 October 2026 12:18



Scottish
Cyber
Coordination
Centre

ConnectWise has shut down customer access to its Cloud Backup service (formerly SkyKick Cloud Backup) after hackers accessed application identities and compromised Microsoft 365 tenants. [...]

Targeted ads installed Candiru spyware in zero-click attacks

BleepingComputer - 16 October 2026 14:20

Candiru spyware was delivered to devices at Al Jazeera Media Network via targeted online advertisements in a zero-click attack that required only rendering the malicious ads on the victim's device. [...]

Attackers Tampered with AOMEI Backupper's Update Servers for Minutes to Deliver a Backdoor

The Hacker News - 16 October 2026 23:13

Attackers repeatedly changed the files that AOMEI Backupper fetches from the vendor's own update servers, in windows of five to ten minutes at a time between May and July 2026, so that any copy of the Windows backup program that checked for an update during one of those windows would download and run a backdoor.

AI Hacking Breach Hits 16 Financial Institutions, Leaks 100,000 Records

Security Magazine - 16 October 2026 13:00

The financial sector was recently targeted by an AI hacking attack.

UK related

Cybersecurity incident at BAE Systems disrupts US bankruptcy court system

CyberScoop - 16 October 2026 16:12

The outage has stopped official bankruptcy notices nationwide since Oct. 9, with no cause or restoration date announced.

NHS data breaches a disgrace, health secretary says

BBC News - 18 October 2026 11:52

A total of 15 NHS staff have been sacked for accessing records of the Nottingham attacks victims.