

Daily Threat Bulletin

14 October 2026

Vulnerabilities

[Ghostscript flaw lets hackers hijack servers via PDF uploads](#)

BleepingComputer - 13 October 2026 18:33

A critical heap buffer overflow vulnerability (CVE-2026-39919) in the Ghostscript interpreter and rendering engine could allow remote code execution through specially crafted PDF files.

[Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days](#)

BleepingComputer - 13 October 2026 16:56

Today is Microsoft's October 2026 Patch Tuesday, with security updates addressing a record-breaking 1,411 flaws, including one actively exploited and two publicly disclosed zero-day vulnerabilities.

[Docker Hub flaw let attackers impersonate users, tamper with images](#)

BleepingComputer - 13 October 2026 12:20

Docker has disclosed a critical vulnerability (CVE-2026-105445) in Docker Hub that let attackers access another user's container repositories using a personal access token (PAT).

[GitLab Patches Max-Severity Vulnerability CVE-2026-97229](#)

Security Affairs - 13 October 2026 14:48

GitLab fixed a critical vulnerability with a maximum CVSS score of 10.0 that could let unauthenticated attackers run code on its servers.

[SAP Discloses Critical CVSS 10 Flaw in Cloud SDK for Python Allowing OAuth2 Credential Theft](#)

The Hacker News - 13 October 2026 23:58

A flaw in SAP's Cloud SDK for Python can send an application's OAuth2 client credentials to a server an attacker controls, SAP said in a security advisory on October 13. The flaw affects multi-tenant applications on SAP Business Technology Platform (BTP) that use the SDK, SAP's official Python client for BTP services.

[CISA Adds Two Known Exploited Vulnerabilities to Catalog](#)

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-96951 Microsoft Windows Command Injection Vulnerability; and CVE-2026-104935 Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability.



Scottish
Cyber
Coordination
Centre

Threat actors and malware

[The MFA Gaps Attackers are Still Exploiting](#)

BleepingComputer - 13 October 2026 11:01

Attackers continue exploiting gaps in MFA coverage, using stolen credentials to access VPNs, RDP, and Windows systems that still rely on passwords alone. Specops explains why protecting cloud applications isn't enough and how organizations can close these authentication gaps.

[Attacker Chains Three Ivanti Connect Secure Zero-Days for Root Access, Only Two Patched So Far](#)

The Hacker News - 14 October 2026 00:03

An attacker chained three zero-day flaws in Ivanti Connect Secure, a VPN appliance, to run commands as root without logging in, security firm Volexity said on October 13.

UK related

[UK Housing Ombudsman Service investigates 'security incident'](#)

BleepingComputer - 13 October 2026 15:19

The U.K. Housing Ombudsman Service is investigating a third-party IT security incident that impacted its case management system on Tuesday.

[AI Turns Familiar Cyberattacks Into a Race Against Time](#)

SecurityWeek - 13 October 2026 12:00

IBM's Steve Wallin talks to SecurityWeek on the effect of AI-driven attacks on enterprise defenses.

[UK Government Announces Sweeping New AI Security Plans](#)

Infosecurity Magazine - 13 October 2026 10:45

The government is planning tweaks to legislation, new incident response and more to head off AI security threats.