Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 September 2026

Vulnerabilities

Adobe fixes critical Magento zero-day exploited to backdoor servers

Bleeping Computer - 08 September 2026 09:34

Adobe has released an emergency fix for CVE-2026-75650, an actively exploited max-severity zero-day vulnerability dubbed StyleSmuggler, that impacts multiple versions of Magento and Adobe Commerce. [...]

FreeIPA Flaw Chain Lets Anonymous Clients Create Reusable Administrator Credentials

The Hacker News - 08 September 2026 16:52

A flaw in FreeIPA lets a client that has never logged in create a Kerberos identity of its own choosing in the directory and end up in the administrators group, Red Hat says.FreeIPA is the system that determines who may log in across a Linux domain and maintains all identities in a 389 Directory Server database accessed via LDAP.

MikroTik Patches Critical Flaws Chained to Hack Routers

Security Week - 08 September 2026 11:15

Dubbed MikroTrick, the bugs allow attackers to bypass authentication, overwrite configuration files, and take over devices.

N-able Patches Critical Zero-Day in N-central

Security Week - 08 September 2026 10:37

Administrators are advised to check their deployments for newly created user accounts they don't recognize.

SAP Security Updates September 2026 – Critical Flaws Patched in SAP NetWeaver, Cloud and Extended Passport

Cyber Security News - 08 September 2026 11:19

SAP has released its September 2026 Security Patch Day updates, delivering 19 new security notes and one update to a previously issued note. The patches address vulnerabilities across SAP NetWeaver, SAP Extended Passport Processing, SAP Cloud Application Programming Model, SAP S/4HANA, SAP Integration Suite, SAP Commerce Cloud, and other enterprise products. The most severe issue [...]

Threat actors and malware

Scottish Cyber Coordination Centre

Hackers build AI frameworks for widescale credential theft

Bleeping Computer - 08 September 2026 08:03

Threat actors are increasingly switching from AI-powered coding assistants to multi-agent frameworks that automate every stage of an attack. [...]

IT Help Desk Impersonation Lets Hackers Bypass MFA

Security Affairs - 08 September 2026 07:41

Attackers bypass endpoint security by posing as IT staff, stealing Microsoft 365 sessions, draining SaaS data and demanding extortion. Forget installing malware because today's extortionists just pick up the phone instead of writing code.

THost9 Android RAT Pairs Packed Loader With ADB Worm

Infosecurity Magazine - 08 September 2026 11:15

THost9 hides its payload and uses ADB to spread across exposed Android devices and containers

BigBear 2 PhaaS Campaign Steals 5000+ Microsoft Credentials

Infosecurity Magazine - 08 September 2026 09:45

CloudSEK has uncovered BigBear 2.0, a new phishing-as-a-service operation targeting Microsoft 365

Hackers Disable Endpoint Protection and Deploy Sliver Across Compromised Windows Domain

Cyber Security News - 08 September 2026 12:10

A new intrusion campaign shows how quickly a Windows domain can be turned into a launchpad for deeper compromise. The operators used a Sliver command-and-control beacon, account creation, credential theft and remote administration to establish control after gaining an initial foothold. The activity was staged from an exposed server and aimed at one unnamed US [...]

U.S. Offers $10 Million Reward for Iranian IRGC Cyber Chief Linked to Critical Infrastructure Attacks

Cyber Security News - 08 September 2026 09:14

The U.S. Department of State's Rewards for Justice program has announced a reward of up to $10 million for information leading to the identification or whereabouts of Amir Yaryab, a senior figure in Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC). U.S. officials allege that Yaryab oversees the command's Cyber Operations Command, managing cyber units [...]

BigBear 2.0 Evilginx2 Phishing Campaign Bypasses Microsoft 365 MFA With Session Cookie Theft

Cyber Security News - 08 September 2026 08:33

Scottish Cyber Coordination Centre

BigBear 2.0 is a phishing operation designed to steal proof that a user has already passed multi-factor authentication. It targets Microsoft 365 accounts through convincing sign-in links, then takes over the logged-in browser session rather than attempting to break the authentication factor. The operation is a rebranded Evilginx2 phishing framework that targets Microsoft 365 accounts. [...]