Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 September 2025

Vulnerabilities

Multiple Apps on Google's Firebase Platform Exposing Sensitive Data

GBHackers - 24 September 2025

A comprehensive security analysis has revealed a widespread vulnerability affecting Firebase-powered mobile applications, with over 150 popular apps inadvertently exposing sensitive user data through misconfigured Google Firebase services.

New Supermicro BMC flaws can create persistent backdoors

BleepingComputer - 24 September 2025 17:13

Two vulnerabilities affecting the firmware of Supermicro hardware, including Baseboard Management Controller (BMC) allow attackers to update systems with maliciously crafted images. [...]

Cisco warns of IOS zero-day vulnerability exploited in attacks

BleepingComputer - 24 September 2025 13:52

Cisco has released security updates to address a high-severity zero-day vulnerability in Cisco IOS and IOS XE Software that is currently being exploited in attacks. [...]

Unpatched flaw in OnePlus phones lets rogue apps text messages

BleepingComputer - 24 September 2025 12:48

A vulnerability in multiple OnePlus OxygenOS versions allows any installed app to access SMS data and metadata without requiring permission or user interaction. [...]

SolarWinds fixed a critical RCE flaw in its Web Help Desk software

Security Affairs - 24 September 2025 12:50

SolarWinds fixed a critical flaw in its Web Help Desk software that could allow attackers to execute arbitrary commands on vulnerable systems. SolarWinds has released hot fixes to address a critical flaw, tracked as CVE-2025-26399 (CVSS score: 9.8), affecting its Web Help Desk software. An attacker could exploit the flaw to execute arbitrary commands on susceptible [...]

Two Critical Flaws Uncovered in Wondershare RepairIt Exposing User Data and AI Models

The Hacker News - 24 September 2025 20:25

Cybersecurity researchers have disclosed two security flaws in Wondershare RepairIt that exposed private user data and potentially exposed the system to artificial intelligence (AI)

model tampering and supply chain risks.The critical-rated vulnerabilities in question, discovered by Trend Micro, are listed below -CVE-2025-10643 (CVSS score: 9.1) - An authentication bypass vulnerability that

Threat actors and malware

Obscura, an obscure new ransomware variant

BleepingComputer - 24 September 2025 11:01

Huntress analysts discovered a previously unseen ransomware variant, Obscura, spreading from a victim company's domain controller. Learn how Obscura works—and what it means for defenders—in this week's Tradecraft Tuesday. [...]

PyPI urges users to reset credentials after new phishing attacks

BleepingComputer - 24 September 2025 10:15

The Python Software Foundation has warned victims of a new wave of phishing attacks using a fake Python Package Index (PyPI) website to reset credentials. [...]

Nation-State hackers exploit Libraesva Email Gateway flaw

Security Affairs - 24 September 2025 15:29

State-sponsored hackers exploited a vulnerability, tracked as CVE-2025-59689, in Libraesva Email Gateway via malicious attachments. Nation-state actors exploited a command injection flaw, tracked as CVE-2025-59689, in Libraesva Email Security Gateway. Libraesva Email Security Gateway is an advanced secure email gateway (SEG) solution developed by the Italian cybersecurity company Libraesva. It's designed to protect organizations against [...]

New YiBackdoor Malware Shares Major Code Overlaps with IcedID and Latrodectus

The Hacker News - 24 September 2025 17:58

Cybersecurity researchers have disclosed details of a new malware family dubbed YiBackdoor that has been found to share "significant" source code overlaps with IcedID and Latrodectus."The exact connection to YiBackdoor is not yet clear, but it may be used in conjunction with Latrodectus and IcedID during attacks," Zscaler ThreatLabz said in a Tuesday report. "YiBackdoor is able to execute

Hackers Exploit Pandoc CVE-2025-51591 to Target AWS IMDS and Steal EC2 IAM Credentials

The Hacker News - 24 September 2025 13:45

Cloud security company Wiz has revealed that it uncovered in-the-wild exploitation of a security flaw in a Linux utility called Pandoc as part of attacks designed to infiltrate Amazon Web Services (AWS) Instance Metadata Service (IMDS).The vulnerability in question is CVE-2025-51591 (CVSS score: 6.5), which refers to a case of Server-Side Request Forgery (SSRF) that allows attackers to

CISA: Attackers Breach Federal Agency via Critical GeoServer Flaw

darkreading - 24 September 2025 22:20

Threat actors exploited CVE-2024-36401 less than two weeks after it was initially disclosed and used it to gain access to a large federal civilian executive branch (FCEB) agency that uses the geospatial mapping data.

Threat Actor Deploys 'OVERSTEP' Backdoor in Ongoing SonicWall SMA Attacks

darkreading - 24 September 2025 14:00

Hackers tracked as UNC6148 are attacking SonicWall security devices by installing hidden software, allowing them to control systems, steal passwords, and hide their activities.

New string of phishing attacks targets Python developers

The Register - 24 September 2025 20:14

If you recently got an email asking you to verify your credentials to a PyPI site, better change that password The Python Software Foundation warned users of a new string of phishing attacks using a phony Python Package Index (PyPI) website and asking victims to verify their account or face suspension, and advised anyone who did provide their credentials to change their password "immediately."...

UK related

UK arrests suspect for RTX ransomware attack causing airport disruptions

BleepingComputer - 24 September 2025 10:55

The UK's National Crime Agency has arrested a suspect linked to a ransomware attack that is causing widespread disruptions across European airports. [...]