Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 June 2026

Vulnerabilities

Apple fixes Beats Studio Buds flaw that let hackers spy on conversations

BleepingComputer - 18 June 2026 09:23

Apple has released security updates to patch a high-severity flaw affecting the Beats Studio Buds wireless earbuds that could allow attackers in Bluetooth range to spy on users' conversations. [...]

Cisco fixed a critical ISE vulnerability that lets attackers to gain root access

Security Affairs - 18 June 2026 17:11

Cisco addressed CVE-2026-20181, a critical ISE vulnerability that lets authenticated admins execute commands and gain root access. Cisco addressed a critical command execution vulnerability, tracked as CVE-2026-20181 (CVSS score of 9.1), affecting Identity Services Engine (ISE) and ISE-PIC.

F5 Patches Two Critical NGINX Open Source Flaws Enabling Remote Code Execution

The Hacker News - 19 June 2026 00:02

F5 has released security updates to address two critical security flaws in NGINX Open Source that could be exploited to achieve code execution on affected systems.The vulnerabilities are listed below - CVE-2026-42530 (CVSS v4 score: 9.2) - A use-after-free vulnerability in the ngx_http_v3_module that could be triggered by a remote unauthenticated attacker when NGINX Open Source is

Splunk Enterprise Vulnerability Exploited in Attacks Days After Disclosure

SecurityWeek - 19 June 2026 05:10

CISA has given federal agencies only three days to patch CVE-2026-20253, which can be exploited for unauthenticated remote code execution.

Atlassian, Splunk Patch Critical Vulnerabilities

SecurityWeek - 18 June 2026 11:59

Splunk patched an OS command injection in AI Toolkit, while Atlassian fixed dozens of flaws in third-party dependencies.

Threat actors and malware

Alert: NCSC issues advice following global targeting of Fortinet firewalls and VPN gateways

NCSC - 18 June 2026 13:00

Scottish Cyber Coordination Centre

Organisations using Fortinet services are being urged to take action following a campaign affecting firewalls and VPN gateways.

USB worm spreads crypto-stealing malware via Windows shortcut files

BleepingComputer - 18 June 2026 13:20

Threat actors targeting cryptocurrency wallets have been distributing clipboard-stealing malware with self-spreading capabilities and using the Tor network to conceal communication. [...]

Klue OAuth breach linked to 'Icarus' Salesforce data theft attacks

BleepingComputer - 18 June 2026 11:19

Market intelligence platform Klue suffered a OAuth breach that enabled the "Icarus" threat actors to steal Salesforce CRM data from multiple organizations in an ongoing extortion campaign. [...]

Microsoft Details Windows Clipper Malware Campaign Using USB LNK Worm and Tor-Based C2

The Hacker News - 18 June 2026 21:00

Microsoft has disclosed details of a Windows-based cryptocurrency clipper campaign that has targeted users since February 2026 with clipboard-intercepting malware with self-spreading capabilities and using the Tor anonymity network to hide communication.

DragonForce Hackers Abuse Microsoft Teams Relays to Hide Backdoor.Turn C2 Traffic

The Hacker News - 18 June 2026 20:00

Threat actors associated with the DragonForce ransomware have been observed using a custom Go-based remote access trojan (RAT) called Backdoor.Turn to conceal command-and-control (C2) traffic inside Microsoft Teams relay infrastructure.

Chinese Hackers Targeting AI, Cyber and National Defense Research

Security Magazine - 18 June 2026 13:20

The campaign was undetected for more than one year.

UK related

Hostile States Behind 75% of Cyber-Attacks on UK Critical Infrastructure, NCSC Warns

Infosecurity Magazine - 18 June 2026 10:10

Richard Horne, the NCSC CEO, said three-quarters of cyber-attacks targeting UK critical infrastructure came from nation-state actors