Scottish Cyber Coordination Centre

Daily Threat Bulletin

31 March 2026

Vulnerabilities

Exploitation of Fresh Citrix NetScaler Vulnerability Begins

SecurityWeek - 30 March 2026 10:24

The critical-severity flaw leaks application memory and can be exploited to obtain authenticated administrative session IDs.

Hackers exploiting critical F5 BIG-IP flaw in attacks, patch now

BleepingComputer - 30 March 2026 07:59

F5 has reclassified a BIG-IP APM denial-of-service (DoS) vulnerability as a critical-severity remote code execution (RCE) flaw, warning that attackers are exploiting it to deploy webshells on unpatched devices.

Critical Fortinet FortiClient EMS flaw exploited for Remote Code Execution

Security Affairs - 30 March 2026 11:43

A critical Fortinet FortiClient EMS vulnerability, tracked as CVE-2026-21643 (CVSS score of 9.1), is now being actively exploited. Defused researchers warn that threat actors are exploiting the vulnerability in Fortinet's FortiClient EMS platform.

OpenAI Patches ChatGPT Data Exfiltration Flaw and Codex GitHub Token Vulnerability

The Hacker News - 31 March 2026 00:35

A previously unknown vulnerability in OpenAI ChatGPT allowed sensitive conversation data to be exfiltrated without user knowledge or consent, according to new findings from Check Point.

Threat actors and malware

Russia-linked APT TA446 uses DarkSword exploit to target iPhone users in phishing wave

Security Affairs - 30 March 2026 08:34

Russia-linked APT group TA446 (aka SEABORGIUM, ColdRiver, Callisto, and Star Blizzard) is using the DarkSword exploit kit in targeted spear-phishing campaigns against iOS devices. The attacks rely on malicious emails to compromise iPhones, highlighting a growing threat from advanced state-sponsored actors.

Scottish Cyber Coordination Centre

DeepLoad Malware Uses ClickFix and WMI Persistence to Steal Browser Credentials

The Hacker News - 30 March 2026 22:17

A new campaign has leveraged the ClickFix social engineering tactic as a way to distribute a previously undocumented malware loader referred to as DeepLoad.

New RoadK1ll WebSocket implant used to pivot on breached networks

BleepingComputer - 30 March 2026 17:49

A newly identified malicious implant named RoadK1ll is enabling threat actors to quietly move from a compromised host to other systems on the network.