Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 April 2026

Vulnerabilities

NCSC Urges Immediate Patching of F5 BIG-IP Bug

Infosecurity Magazine - 31 March 2026 09:45

The National Cyber Security Centre wants UK firms to patch CVE-2025-53521

Exploitation of Critical Fortinet FortiClient EMS Flaw Begins

SecurityWeek - 31 March 2026 12:39

The SQL injection vulnerability allows unauthenticated attackers to execute arbitrary code remotely, via crafted HTTP requests.

GIGABYTE Control Center vulnerable to arbitrary file write flaw

BleepingComputer - 31 March 2026 19:28

The GIGABYTE Control Center is vulnerable to an arbitrary file-write flaw that could allow a remote, unauthenticated attacker to access files on vulnerable hosts.

Threat actors and malware

Axios Supply Chain Attack Pushes Cross-Platform RAT via Compromised npm Account

The Hacker News - 31 March 2026 12:38

The popular HTTP client known as Axios has suffered a supply chain attack after two newly published versions of the npm package introduced a malicious dependency that delivers a trojan capable of targeting Windows, macOS, and Linux systems.

Cisco source code stolen in Trivy-linked dev environment breach

BleepingComputer - 31 March 2026 14:53

Cisco has suffered a cyberattack after threat actors used stolen credentials from the recent Trivy supply chain attack to breach its internal development environment and steal source code belonging to the company and its customers.

Google Drive ransomware detection now on by default for paying users

BleepingComputer - 01 April 2026 03:35

Google announced that the AI-powered Google Drive ransomware detection feature has reached general availability and is now enabled by default for all paying users.

Scottish Cyber Coordination Centre

StrongSwan Flaw Allows Unauthenticated Attackers to Crash VPNs

SecurityWeek - 31 March 2026 11:21

Remotely exploitable, the integer underflow vulnerability impacts StrongSwan releases spanning 15 years.