Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 May 2026

Vulnerabilities

Chaotic Eclipse discloses MiniPlasma zero-day, suggesting a missing or undone 2020 Windows security fix

Security Affairs - 18 May 2026 09:13

MiniPlasma: a Windows SYSTEM privilege escalation believed patched in 2020 (CVE-2020-17103) is still fully working on every patched Windows 11. Once again, security researcher Chaotic Eclipse has released a proof-of-concept exploit for a new Windows privilege escalation zero-day called MiniPlasma, which can grant attackers SYSTEM privileges on fully patched systems.

Ivanti, Fortinet, SAP, VMware, n8n Patch RCE, SQL Injection, Privilege Escalation Flaws

The Hacker News - 18 May 2026 17:24

Ivanti, Fortinet, n8n, SAP, and VMware have released security fixes for various vulnerabilities that could be exploited by bad actors to bypass authentication and execute arbitrary code.

'Claw Chain' Vulnerabilities Threaten OpenClaw Deployments

darkreading - 18 May 2026 22:24

The now patched vulnerabilities in the rapidly growing AI agent framework allow attackers to steal credentials, escalate privileges, and maintain persistence.

Torvalds Offers Guidance as AI Bug Reports Clog Up Linux Security Workflow

Security Boulevard - 18 May 2026 20:22

Linux kernel maintainers are confronting a new operational problem tied to the rapid adoption of AI-assisted coding tools, as too many people are reporting the same vulnerabilities at the same time.

Threat actors and malware

INTERPOL 'Operation Ramz' seizes 53 malware, phishing servers

BleepingComputer - 18 May 2026 19:15

More than 200 individuals were arrested for cybercrime activities during INTERPOL's Operation Ramz, which focused on the Middle East and North Africa. [...]

Leaked Shai-Hulud malware fuels new npm infostealer campaign

Scottish Cyber Coordination Centre

BleepingComputer - 18 May 2026 14:28

The Shai-Hulud malware leaked last week is now used in new attacks on the Node Package Manager (npm) index, as infected packages emerged over the weekend. [...]

Grafana says stolen GitHub token let hackers steal codebase

BleepingComputer - 18 May 2026 10:46

Grafana Labs disclosed that hackers have downloaded its source code after breaching its GitHub environment using a stolen access token. [...]

Microsoft Exchange Zero-Day Under Attack, No Patch Available

darkreading - 18 May 2026 22:43

CVE-2026-42897 stems from a cross-site scripting (XSS) vulnerability and can allow an attacker to compromise Outlook Web Access (OWA) mailboxes.