Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 April 2026

Vulnerabilities

Microsoft releases emergency patches for critical ASP.NET flaw

BleepingComputer - 22 April 2026 05:08

Microsoft has released out-of-band (OOB) security updates to patch a critical ASP.NET Core privilege escalation vulnerability.

Mirai Botnet exploits CVE-2025-29635 to target legacy D-Link routers

Security Affairs - 22 April 2026 18:31

Mirai botnet is targeting old D-Link routers using CVE-2025-29635, a command injection flaw exploitable via crafted POST requests after public PoC disclosure.

Critical BRIDGE:BREAK flaws impact Lantronix and Silex Technology converters

Security Affairs - 22 April 2026 14:29

Researchers at Forescout Research Vedere Labs found 22 BRIDGE:BREAK flaws in serial-to-IP devices from Lantronix and Silex Technology. Serial-to-IP converters, also known as serial device servers, connect legacy serial equipment to modern IP networks for remote monitoring.

Oracle Patches 450 Vulnerabilities With April 2026 CPU

SecurityWeek - 22 April 2026 09:41

The company released 481 new security patches across 28 product families, including over 300 fixes for remotely exploitable, unauthenticated flaws.

Claude Mythos Finds 271 Firefox Vulnerabilities

SecurityWeek - 22 April 2026 12:27

All the flaws could have also been found by an elite human researcher, according to Mozilla.

Threat actors and malware

Kyber ransomware gang toys with post-quantum encryption on Windows

BleepingComputer - 22 April 2026 15:52

A new Kyber ransomware operation is targeting Windows systems and VMware ESXi endpoints in recent attacks, with one variant implementing Kyber1024 post-quantum encryption.

Scottish Cyber Coordination Centre

New npm supply-chain attack self-spreads to steal auth tokens

BleepingComputer - 22 April 2026 09:57

A new supply chain attack targeting the Node Package Manager (npm) ecosystem is stealing developer credentials and attempting to spread through packages published from compromised accounts.

New GoGra malware for Linux uses Microsoft Graph API for comms

BleepingComputer - 22 April 2026 07:00

A Linux variant of the GoGra backdoor uses legitimate Microsoft infrastructure, relying on an Outlook inbox for stealthy payload delivery.

NCSC Unveils SilentGlass, a Plug-In Device to Protect Monitors from Cyber-Attacks

Infosecurity Magazine - 22 April 2026 16:00

The UK's cybersecurity agency said the devices will be available for purchase by organizations around the world.

CyberUK

Most Serious Cyberattacks Against the UK Now From Russia, Iran and China, Cyber Chief Says

SecurityWeek - 22 April 2026 13:57

British businesses need to prepare themselves to defend against cyberattacks because the U.K. could be targeted "at scale," if it became involved in an international conflict.

UK Commits £90m for Cybersecurity and Pushes for 'Resilience Pledge'

Infosecurity Magazine - 22 April 2026 15:10

UK unveils £90m cybersecurity funding at CYBERUK to boost SME resilience, promote Cyber Essentials and a new Cyber Resilience Pledge, sparking industry debate.

UK cyber agency handling four major incidents a week as nation-state attacks surge

The Record from Recorded Future News - 22 April 2026 13:45

Britain's cybersecurity chief warned Tuesday that the country is handling four nationally significant cyber incidents every week, with the majority now traced back to hostile foreign governments rather than criminal hackers.