Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 March 2026

Vulnerabilities

Citrix Urges Patching Critical NetScaler Flaw Allowing Unauthenticated Data Leaks

The Hacker News - 24 March 2026 12:29

Citrix has released security updates to address two vulnerabilities in NetScaler ADC and NetScaler Gateway, including a critical flaw that could be exploited to leak sensitive data from the application.

PTC warns of imminent threat from critical Windchill, FlexPLM RCE bug

BleepingComputer - 24 March 2026 20:04

PTC Inc. is warning of a critical vulnerability in Windchill and FlexPLM, widely used product lifecycle management (PLM) solutions, that could allow remote code execution.

Chrome 146 Update Patches High-Severity Vulnerabilities

SecurityWeek - 24 March 2026 14:35

The software refresh fixes eight memory safety bugs affecting seven Chrome components.

Threat actors and malware

1K+ cloud environments infected following Trivy supply chain attack

The Register - 24 March 2026 21:31

Thousands of organizations' cloud environments have been infected with secret-stealing malware as a result of the Trivy supply-chain attack last week, and now the criminals that compromised the open source scanners are working with notorious extortion crews like Lapsus$.

TeamPCP Hacks Checkmarx GitHub Actions Using Stolen CI Credentials

The Hacker News - 24 March 2026 17:08

Two more GitHub Actions workflows have become the latest to be compromised by credential-stealing malware by a threat actor known as TeamPCP, the cloud-native cybercriminal operation also behind the Trivy supply chain attack.

Scottish Cyber Coordination Centre

North Korea-linked threat actors abuse VS Code auto-run to spread StoatWaffle malware

Security Affairs - 24 March 2026 08:09

North Korea-linked threat actor Team 8 behind the Contagious Interview campaign is spreading StoatWaffle malware through malicious Microsoft Visual Studio Code projects.

HackerOne slams supplier for delayed breach notice after staff data exposed

The Register - 24 March 2026 14:27

Almost 300 HackerOne employees are caught up in a data breach, with the bug bounty business slamming a third-party benefits provider for a weeks-long delay in notification.

Stryker says malware was involved in recent cyberattack as production lines reopen

The Record from Recorded Future News - 24 March 2026 21:45

The medical device firm Stryker said it is ramping production lines back up two weeks after alleged Iranian cyber actors wiped more than 200,000 company devices.

RSA Conference: UK NCSC Head Urges Industry to Develop Vibe Coding Safeguards

Infosecurity Magazine - 24 March 2026 22:00

The head of the UK's NCSC is calling the cybersecurity industry to "seize the disruptive vibe coding opportunity" to make software more secure