Scottish Cyber Coordination Centre

# Daily Threat Bulletin

13 May 2026

## Vulnerabilities

### Fortinet warns of critical RCE flaws in FortiSandbox and FortiAuthenticator

BleepingComputer - 12 May 2026 15:23

Fortinet has released security patches for two critical vulnerabilities in FortiSandbox and FortiAuthenticator that could enable attackers to run commands or arbitrary code. [...]

### Microsoft May 2026 Patch Tuesday fixes 120 flaws, no zero-days

BleepingComputer - 12 May 2026 15:08

Today is Microsoft's May 2026 Patch Tuesday, with security updates for 120 flaws and no zero-days disclosed this month. [...]

### SAP fixes critical vulnerabilities in Commerce Cloud and S/4HANA

BleepingComputer - 12 May 2026 08:04

SAP has released the May 2026 security updates addressing 15 vulnerabilities across multiple products, including two critical flaws in the Commerce Cloud enterprise-grade e-commerce platform and the S/4HANA ERP suite. [...]

### Attackers exploit cPanel CVE-2026-41940 to deploy Filemanager Backdoor

Security Affairs - 12 May 2026 12:41

Attackers are exploiting cPanel flaw CVE-2026-41940 to install the Filemanager backdoor and gain unauthorized admin access. Cybercriminals are actively exploiting the critical cPanel vulnerability CVE-2026-41940 (CVSS score of 9.3) to deploy a backdoor called Filemanager on compromised servers.

### New Exim BDAT Vulnerability Exposes GnuTLS Builds to Potential Code Execution

The Hacker News - 12 May 2026 23:14

Exim has released security updates to address a severe security issue affecting certain configurations that could enable memory corruption and potential code execution.Exim is an open-source Mail Transfer Agent (MTA) designed for Unix-like systems to receive, route, and deliver email.

### OpenAI Launches Daybreak for AI-Powered Vulnerability Detection and Patch Validation

The Hacker News - 12 May 2026 13:25

Scottish Cyber Coordination Centre

OpenAI has launched Daybreak, a new cybersecurity initiative that brings together frontier artificial intelligence (AI) model capabilities and Codex Security to help organizations identify and patch vulnerabilities before attackers find a way in using the same issues.

## Threat actors and malware

### CC-4781 - Supply Chain Attack Affecting Numerous npm and PyPI Packages

NHS Digital - 12 May 2026 15:58

Severity: Medium A supply chain attack, dubbed as “Mini Shai-Hulud”, is affecting well-known projects including TanStack, Mistral AI, UiPath, and OpenSearch A supply chain attack, dubbed as “Mini Shai-Hulud”, is affecting well-known projects including TanStack, Mistral AI, UiPath, and OpenSearch.

### Signal adds security warnings for social engineering, phishing attacks

BleepingComputer - 12 May 2026 16:40

Signal has introduced new in-app confirmations and warning messages as additional safeguards against phishing and social engineering attempts that could lead to various forms of fraud. […]

### Instructure Reaches Ransom Agreement with ShinyHunters to Stop 3.65TB Canvas Leak

The Hacker News - 12 May 2026 14:07

American educational technology company Instructure, the parent company of Canvas, said it reached an “agreement” with a decentralized cybercrime extortion group after it breached its network and threatened to leak stolen information from thousands of schools and universities.

### TeamPCP Compromises Checkmarx Jenkins AST Plugin Weeks After KICS Supply Chain Attack

The Hacker News - 12 May 2026 01:00

Checkmarx has confirmed that a modified version of the Jenkins AST plugin was published to the Jenkins Marketplace.”If you are using Checkmarx Jenkins AST plugin, you need to ensure that you are using the version 2.0.13-829.vc72453fa_1c16 that was published on December 17, 2025 or previously,” the cybersecurity company said in a statement over the weekend.

### Hackers Used AI to Develop First Known Zero-Day 2FA Bypass for Mass Exploitation

The Hacker News - 11 May 2026 22:15

Google on Monday disclosed that it identified an unknown threat actor using a zero-day exploit that it said was likely developed with an artificial intelligence (AI) system, marking the first time the technology has been put to use in the wild in a malicious context for vulnerability discovery and exploit generation.

### Fake Claude search results lure Mac users into ClickFix attack

Scottish Cyber Coordination Centre

Malwarebytes - 12 May 2026 16:46

Researchers found a ClickFix campaign that uses fake Claude setup guides to trick Mac users into infecting themselves.