



# Daily Threat Bulletin

6 January 2025

## Vulnerabilities

### [New n8n Vulnerability \(9.9 CVSS\) Lets Authenticated Users Execute System Commands](#)

The Hacker News - 06 January 2026 11:38

A new critical security vulnerability has been disclosed in n8n, an open-source workflow automation platform, that could enable an authenticated attacker to execute arbitrary system commands on the underlying host.

### [Critical AdonisJS Bodyparser Flaw \(CVSS 9.2\) Enables Arbitrary File Write on Servers](#)

The Hacker News - 06 January 2026 10:00

Users of the “@adonisjs/bodyparser” npm package are being advised to update to the latest version following the disclosure of a critical security vulnerability that, if successfully exploited, could allow a remote attacker to write arbitrary files on the server.

### [Critical ‘MongoBleed’ Bug Under Active Attack, Patch Now](#)

darkreading - 05 January 2026 21:52

A memory leak security vulnerability allows unauthenticated attackers to extract passwords and tokens from MongoDB servers.

## Threat actors and malware

### [Cloud file-sharing sites targeted for corporate data theft attacks](#)

BleepingComputer - 05 January 2026 18:52

A threat actor known as Zestix has been offering to corporate data stolen from dozens of companies likely after breaching their ShareFile, Nextcloud, and OwnCloud instances. [...]

### [ClickFix attack uses fake Windows BSOD screens to push malware](#)

BleepingComputer - 05 January 2026 17:16

A new ClickFix social engineering campaign is targeting the hospitality sector in Europe, using fake Windows Blue Screen of Death (BSOD) screens to trick users into manually compiling and executing malware on their systems. [...]

### [VSCode IDE forks expose users to “recommended extension” attacks](#)

BleepingComputer - 05 January 2026 12:41



Scottish  
Cyber  
Coordination  
Centre

Popular AI-powered integrated development environment solutions, such as Cursor, Windsurf, Google Antigravity, and Trae, recommend extensions that are non-existent in the OpenVSX registry, allowing threat actors to claim the namespace and upload malicious extensions. [...]

### **NordVPN denies breach claims, says attackers have “dummy data”**

BleepingComputer - 05 January 2026 10:48

NordVPN denied allegations that its internal Salesforce development servers were breached, saying that cybercriminals obtained “dummy data” from a trial account on a third-party automated testing platform. [...]

### **New VVS Stealer Malware Targets Discord Accounts via Obfuscated Python Code**

The Hacker News - 05 January 2026 14:18

Cybersecurity researchers have disclosed details of a new Python-based information stealer called VVS Stealer (also styled as VVS \$tealer) that’s capable of harvesting Discord credentials and tokens. The stealer is said to have been on sale on Telegram as far back as April 2025, according to a report from Palo Alto Networks Unit 42.

## **UK related**

[Cyberattack forces British high school to close](#)

The Record from Recorded Future News - 05 January 2026 16:45