



# Daily Threat Bulletin

8 January 2026

## Vulnerabilities

### [CISA Adds Two Known Exploited Vulnerabilities to Catalog](#)

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2009-0556 Microsoft Office PowerPoint Code Injection Vulnerability

CVE-2025-37164 HPE OneView Code Injection Vulnerability

### [Hackers Exploit Zero-Day in Discontinued D-Link Devices](#)

SecurityWeek - 07 January 2026 13:33

The critical-severity vulnerability allows unauthenticated, remote attackers to execute arbitrary shell commands.

### [Critical n8n Vulnerability \(CVSS 10.0\) Allows Unauthenticated Attackers to Take Full Control](#)

The Hacker News - 07 January 2026 20:18

Cybersecurity researchers have disclosed details of yet another maximum-severity security flaw in n8n, a popular workflow automation platform, that allows an unauthenticated remote attacker to gain complete control over susceptible instances.

### [Veeam resolves CVSS 9.0 RCE flaw and other security issues](#)

Security Affairs - 07 January 2026 12:31

Veeam released patches for multiple Backup & Replication flaws, including a critical RCE vulnerability tracked as CVE-2025-59470 (CVSS score of 9.0). A Backup or Tape Operator can achieve remote code execution as the postgres user by abusing malicious interval or order parameters.

### [Critical jsPDF flaw lets hackers steal secrets via generated PDFs](#)

BleepingComputer - 07 January 2026 17:46

The jsPDF library for generating PDF documents in JavaScript applications is vulnerable to a critical vulnerability that allows an attacker to steal sensitive data from the local filesystem by including it in generated files.



### **Complex Routing, Misconfigurations Exploited for Domain Spoofing in Phishing Attacks**

SecurityWeek - 07 January 2026 12:29

Threat actors spoof legitimate domains to make their phishing emails appear to have been sent internally.

### **[R1] Nessus Agent Versions 11.0.3 and 10.9.3 Fix One Vulnerability**

Tenable Product Security Advisories - 07 January 2026 14:47

A vulnerability has been identified in the installation/uninstallation of the Nessus Agent Tray App on Windows Hosts which could lead to escalation of privileges.

## **Threat actors and malware**

### **Black Cat Behind SEO Poisoning Malware Campaign Targeting Popular Software Searches**

The Hacker News - 07 January 2026 23:39

A cybercrime gang known as Black Cat has been attributed to a search engine optimization (SEO) poisoning campaign that employs fraudulent sites advertising popular software to trick users into downloading a backdoor capable of stealing sensitive data.

### **Microsoft Warns Misconfigured Email Routing Can Enable Internal Domain Phishing**

The Hacker News - 07 January 2026 16:12

Threat actors engaging in phishing attacks are exploiting routing scenarios and misconfigured spoof protections to impersonate organizations' domains and distribute emails that appear as if they have been sent internally.

### **Versatile Malware Loader pkr\_mtsi Delivers Diverse Payloads**

Infosecurity Magazine - 07 January 2026 17:45

Malicious Windows packer named pkr\_mtsi used as a flexible malware loader in malvertising campaigns.

### **Ghost Tap Malware Fuels Surge in Remote NFC Payment Fraud**

Infosecurity Magazine - 07 January 2026 17:00

New Android malware enables unauthorized tap-to-pay transactions without physical access to bank cards.



Scottish  
Cyber  
Coordination  
Centre

## UK incidents

### [UK announces plan to strengthen public sector cyber defenses](#)

BleepingComputer - 07 January 2026 08:15

The United Kingdom has announced a new cybersecurity strategy, backed by more than £210 million (\$283 million), to boost cyber defenses across government departments and the wider public sector.

### [Cyberattack forces British high school to cancel classes and delay reopening](#)

The Record from Recorded Future News - 07 January 2026 13:56

Higham Lane School in Nuneaton, shuttered by a cyberattack over the Christmas holiday, has pushed back its reopening date due to the challenges posed by the incident.

### [Ministry of Justice splurged £50M on security – still missed Legal Aid Agency cyberattack](#)

The Register - 07 January 2026 13:28

The UK's Ministry of Justice spent £50 million (\$67 million) on cybersecurity improvements at the Legal Aid Agency (LAA) before the high-profile cyberattack it disclosed last year.