



Scottish  
Cyber  
Coordination  
Centre

# Daily Threat Bulletin

21 September 2026

## Vulnerabilities

### [Click2Shell WordPress Flaw Lets Attackers Gain RCE With a Single Malicious Link](#)

Cyber Security News - 19 September 2026 05:30

WordPress administrators are being urged to update after researchers disclosed Click2Shell, an exploit chain that can turn one malicious link into remote code execution (RCE) on a vulnerable website.

### [Critical Microsoft Azure AI Foundry Vulnerability Allows Attackers to Escalate Privileges](#)

Cyber Security News - 18 September 2026 15:14

Microsoft has patched a maximum-severity security flaw in Azure AI Foundry, its enterprise platform for building and managing generative AI applications and agents, that could have allowed an unauthenticated attacker to escalate privileges over the network without any user interaction.

### [Check Point Fixes Critical CVE-2026-91843 Allowing Root Code Execution](#)

Security Affairs - 18 September 2026 08:52

Check Point fixed CVE-2026-91843, a critical flaw that could let attackers run code as root on Security Management and Log Servers with no login needed.

### [SolarWinds Patches ARM Hard-Coded Key Flaw Enabling Unauthenticated RCE](#)

The Hacker News - 19 September 2026 16:01

SolarWinds has released security updates to address a high-severity flaw in Access Rights Manager (ARM) that, if successfully exploited, could lead to an unauthenticated remote code execution vulnerability.

### [Critical Pre-Auth RCE in Orkes Conductor Workflow Platform Exploited in the Wild](#)

The Hacker News - 19 September 2026 14:48

A critical vulnerability impacting Orkes Conductor is being actively exploited in the wild, according to Fortinet. The vulnerability in question is CVE-2026-58138 (CVSS v3.1 score: 9.8/CVSS v4 score: 9.3), which relates to a case of unauthenticated remote code execution.

### [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-2025-39964 Linux Kernel Race Condition



Scottish  
Cyber  
Coordination  
Centre

Vulnerability CVE-2026-53266 Linux Kernel Out-of-Bounds Write Vulnerability These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risks to the federal enterprise.

## Threat actors and malware

### **TanStack Supply Chain Attack Lets Hackers Steal 170 Private CrowdSec GitHub Repositories**

Cyber Security News - 19 September 2026 12:21

CrowdSec has disclosed that attackers copied about 170 private GitHub repositories after a former employee's account was compromised through May's TanStack npm supply chain attack.

### **Google Gemini AI Hacked 3 Real Companies during a Cybersecurity Test**

Cyber Security News - 19 September 2026 09:59

Google has confirmed that its Gemini artificial intelligence model accessed protected systems belonging to three companies during a cybersecurity evaluation after a testing error exposed the agent to the public internet.

### **Click2Shell WordPress Flaw Lets Attackers Gain RCE With a Single Malicious Link**

Cyber Security News - 19 September 2026 05:30

WordPress administrators are being urged to update after researchers disclosed Click2Shell, an exploit chain that can turn one malicious link into remote code execution (RCE) on a vulnerable website.

### **BragJack attacks hijack AI browser agents through malicious extensions**

BleepingComputer - 19 September 2026 11:56

BragJack, a proof-of-concept attack from Forever Security's Gal Weizman, hijacks the AI assistants in Chrome, Edge, Opera Neon, Perplexity Comet, and Claude in Chrome using one malicious extension.

### **ShinyHunters hacks Clop leak site, threatens to extort ransomware gang**

BleepingComputer - 19 September 2026 10:48

The ShinyHunters extortion gang breached the Clop (aka ClOp) ransomware operation's data leak site, defacing the Tor site and allegedly stealing server data and the private keys for its onion service. [...]