



# Daily Threat Bulletin

5 December 2025

## Vulnerabilities

### [React2Shell: In-the-Wild Exploitation Expected for Critical React Vulnerability](#)

SecurityWeek - 04 December 2025 11:06

A researcher has pointed out that only instances using a newer feature are impacted by CVE-2025-55182.

### [Hackers are exploiting ArrayOS AG VPN flaw to plant webshells](#)

BleepingComputer - 04 December 2025 19:05

Threat actors have been exploiting a command injection vulnerability in Array AG Series VPN devices to plant webshells and create rogue users.

### [NCSC's 'Proactive Notifications' warns orgs of flaws in exposed devices](#)

BleepingComputer - 04 December 2025 18:21

The UK's National Cyber Security Center (NCSC) announced the testing phase of a new service called Proactive Notifications, designed to inform organizations in the country of vulnerabilities present in their environment.

## Threat actors and malware

### [PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Information Technology Systems](#)

CISA Advisories -

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of ongoing intrusions by People's Republic of China (PRC) state-sponsored cyber actors using BRICKSTORM malware for long-term persistence on victim systems. BRICKSTORM is a sophisticated backdoor for VMware vSphere<sup>1,2</sup> and Windows environments.

### [Predator spyware uses new infection vector for zero-click attacks](#)

BleepingComputer - 04 December 2025 16:47

The Predator spyware from surveillance company Intellexa has been using a zero-click infection mechanism dubbed "Aladdin" that compromised specific targets when simply viewing a malicious advertisement.



Scottish  
Cyber  
Coordination  
Centre

### **Silver Fox Uses Fake Microsoft Teams Installer to Spread ValleyRAT Malware in China**

The Hacker News - 04 December 2025 23:55

The threat actor known as Silver Fox has been spotted orchestrating a false flag operation to mimic a Russian threat group in attacks targeting organizations in China. The search engine optimization (SEO) poisoning campaign leverages Microsoft Teams lures to trick unsuspecting users into downloading a malicious setup file that leads to the deployment of ValleyRAT (Winos 4.0).

### **5 Threats That Reshaped Web Security This Year [2025]**

The Hacker News - 04 December 2025 18:00

As 2025 draws to a close, security professionals face a sobering realization: the traditional playbook for web security has become dangerously obsolete. AI-powered attacks, evolving injection techniques, and supply chain compromises affecting hundreds of thousands of websites forced a fundamental rethink of defensive strategies.