



Daily Threat Bulletin

10 December 2025

Vulnerabilities

[Microsoft December 2025 Patch Tuesday fixes 3 zero-days, 57 flaws](#)

BleepingComputer - 09 December 2025 14:38

Microsoft's December 2025 Patch Tuesday fixes 57 flaws, including one actively exploited and two publicly disclosed zero-day vulnerabilities.

[Fortinet, Ivanti, and SAP Issue Urgent Patches for Authentication and Code Execution Flaws](#)

The Hacker News - 10 December 2025 11:20

Fortinet, Ivanti, and SAP have moved to address critical security flaws in their products that, if successfully exploited, could result in an authentication bypass and code execution. The Fortinet vulnerabilities affect FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager and relate to a case of improper verification of a cryptographic signature.

[Intel, AMD Processors Affected by PCIe Vulnerabilities](#)

SecurityWeek - 10 December 2025 09:02

The PCIe flaws, found by Intel employees, can be exploited for information disclosure, escalation of privilege, or DoS. The post Intel, AMD Processors Affected by PCIe Vulnerabilities appeared first on SecurityWeek.

[Adobe Patches Nearly 140 Vulnerabilities](#)

SecurityWeek - 09 December 2025 21:35

The Experience Manager security update resolves 117 vulnerabilities, including 116 identified as cross-site scripting (XSS) bugs. The post Adobe Patches Nearly 140 Vulnerabilities appeared first on SecurityWeek.

[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-2022-37055 D-Link Routers Buffer Overflow Vulnerability CVE-2025-66644 Array Networks ArrayOS AG OS Command Injection Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise management practice.

[UK NCSC Raises Alarms Over Prompt Injection Attacks](#)

Infosecurity Magazine - 09 December 2025 12:30



Scottish
Cyber
Coordination
Centre

The UK's National Cyber Security Centre has warned of the dangers of comparing prompt injection to SQL injection.

Threat actors and malware

[Ransomware IAB abuses EDR for stealthy malware execution](#)

BleepingComputer - 09 December 2025 11:24

An initial access broker tracked as Storm-0249 is abusing endpoint detection and response solutions and trusted Microsoft Windows utilities to load malware, establish communication, and persistence in preparation for ransomware attacks.

[Four Threat Clusters Using CastleLoader as GrayBravo Expands Its Malware Service Infrastructure](#)

The Hacker News - 09 December 2025 22:31

Four distinct threat activity clusters have been observed leveraging a malware loader known as CastleLoader, strengthening the previous assessment that the tool is offered to other threat actors under a malware-as-a-service (MaaS) model.

[Storm-0249 Escalates Ransomware Attacks with ClickFix, Fileless PowerShell, and DLL Sideloads](#)

The Hacker News - 09 December 2025 20:07

The threat actor known as Storm-0249 is likely shifting from its role as an initial access broker to adopt a combination of more advanced tactics like domain spoofing, DLL side-loading, and fileless PowerShell execution to facilitate ransomware attacks.

[React2Shell Attacks Linked to North Korean Hackers](#)

SecurityWeek - 09 December 2025 16:18

North Korean threat actors are believed to be behind CVE-2025-55182 exploitation delivering EtherRAT. The post React2Shell Attacks Linked to North Korean Hackers appeared first on SecurityWeek.

[Opportunistic Pro-Russia Hacktivists Attack US and Global Critical Infrastructure](#)

CISA Advisories -

CISA, in partnership with Federal Bureau of Investigation, the National Security Agency, Department of Energy, Environmental Protection Agency, the Department of Defense Cyber Crime Center, and other international partners published a joint cybersecurity advisory, Pro-Russia Hacktivists Create Opportunistic Attacks Against US and Global Critical Infrastructure.

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

CISA Advisories -



Scottish
Cyber
Coordination
Centre

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^{1,2} and Windows environments.

UK related

[UK finally vows to look at 35-year-old Computer Misuse Act](#)

The Register - 09 December 2025 11:15

As Portugal gives researchers a pass under cybersecurity law Portugal has become the latest country to carve out protections for researchers under its cybersecurity law. The move increases pressure on the UK Government to update the Computer Misuse Act to protect cybersecurity pros from prosecution.

[UK Sanctions Russian and Chinese Firms Suspected of Being 'Malign Actors' in Information Warfare](#)

SecurityWeek - 10 December 2025 03:31

Britain and its allies face escalating "hybrid threats ... designed to weaken critical national infrastructure, undermine our interests and interfere in our democracies.