Daily brief, Tuesday, February 10, 2026

Feb 9, 7:00 PM to Feb 10, 7:00 PM ET

Generated Nov 7, 2026, 6:13 PM ET

0	6	0	10	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

6 newly exploited, 10 new critical CVEs, 2 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

6

8.8 **CVE-2026-21510** Microsoft Windows CISA KEV

An attacker gains arbitrary code execution with elevated privileges through Microsoft Windows Shell, including Windows Explorer and Windows Search, via a protection mechanism failure.

8.8 **CVE-2026-21513** Microsoft Windows CISA KEV

A remote attacker over the network can bypass a security feature in the MSHTML Framework component of Microsoft Windows due to a protection mechanism failure.

7.8 **CVE-2026-21514** Microsoft Office CISA KEV

Microsoft Office Word flaw from relying on untrusted inputs in a security decision lets an authorized local attacker elevate privileges.

7.8 **CVE-2026-21519** Microsoft Windows CISA KEV

Type confusion in Microsoft Windows Desktop Window Manager lets an authorized local attacker elevate privileges.

7.8 **CVE-2026-21533** Microsoft Windows CISA KEV

An authorized local attacker elevates privileges in Microsoft Windows Remote Desktop Services through improper privilege management.

6.2 **CVE-2026-21525** Microsoft Windows CISA KEV

A NULL pointer dereference in Microsoft Windows Remote Access Connection Manager lets an unauthorized local attacker cause a denial of service.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs 10

9.8 **CVE-2026-21531** Microsoft azure conversation authoring client library
Deserialization of untrusted data in Azure SDK allows an unauthorized attacker to execute code over a network.

9.9 **CVE-2026-0488** Sap netweaver application server abap
An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorized critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a

9.6 **CVE-2026-0509** Sap netweaver as abap kernel
SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated, low-privileged user to perform background Remote Function Calls without the required S_RFC authorization in certain cases. This can result in a high impact on integrity and availa

9.8 **CVE-2026-23906** Apache druid
Affected Products and Versions * Apache Druid * Affected Versions: 0.17.0 through 35.x (all versions prior to 36.0.0) * Prerequisites: * druid-basic-security extension enabled * LDAP authenticator configured * Underlying LDAP server permits anonymous bind Vuln

9.8 **CVE-2026-1774**
CASL Ability, versions 2.4.0 through 6.7.4, contains a prototype pollution vulnerability.

9.8 **CVE-2026-2096** Flowring agentflow
Agentflow developed by Flowring has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents by using a specific functionality.

9.8 **CVE-2026-2095** Flowring agentflow
Agentflow developed by Flowring has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to exploit a specific functionality to obtain arbitrary user authentication token and log into the system as any user.

9.9 **CVE-2026-26009**
Catalyst is a platform built for enterprise game server hosts, game communities, and billing panel integrations. Install scripts defined in server templates execute directly on the host operating system as root via bash -c, with no sandboxing or containerizati

9.8 **CVE-2026-25993** Evershop evershop
EverShop is a TypeScript-first eCommerce platform. During category update and deletion event handling, the application embeds path / request_path values—derived from the url_key stored in the database—into SQL statements via string concatenation and passes the

9.8 **CVE-2025-11242**
Server-Side Request Forgery (SSRF) vulnerability in Teknolist Computer Systems Software Publishing Industry and Trade Inc. Okulistik allows Server Side Request Forgery. This issue affects Okulistik: through 21102025.

Ransomware

No leak-site posts collected.

New data breaches 2

Association Nationale des Premiers Secours	anps.fr	5,600 accounts
Toy Battles	toybattles.net	1,017 accounts

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.