Daily brief, Thursday, November 20, 2025

Nov 19, 7:00 PM to Nov 20, 7:00 PM ET

Generated Nov 9, 2026, 8:13 AM ET

0	0	0	11	0	4
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

11 new critical CVEs, 4 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs

11

9.8 **CVE-2025-59245** Microsoft sharepoint online

Microsoft SharePoint Online Elevation of Privilege Vulnerability

10.0 **CVE-2025-49752** Microsoft azure bastion developer

Azure Bastion Elevation of Privilege Vulnerability

9.8 **CVE-2025-60738** Ilevia eve x1 server firmware DETECTION

An issue in Ilevia EVE X1 Server Firmware Version v4.7.18.0.eden and before Logic Version v6.00 - 2025_07_21 and before allows a remote attacker to execute arbitrary code via the ping.php component does not perform secure filtering on IP parameters

9.3 **CVE-2025-34320**

BASIS BBj versions prior to 25.00 contain a Jetty-served web endpoint that fails to properly validate or canonicalize input path segments. This allows unauthenticated directory traversal sequences to cause the server to read arbitrary system files accessible t

9.8 **CVE-2025-64428** Dataease dataease

Dataease is an open source data visualization analysis tool. Versions prior to 2.10.17 are vulnerable to JNDI injection. A blacklist was added in the patch for version 2.10.14. However, JNDI injection remains possible via the iiop, corbaname, and iiopname sche

9.8 **CVE-2025-63888** Thinkphp thinkphp

The read function in file thinkphp\library\think\template\driver\File.php in ThinkPHP 5.0.24 contains a remote code execution vulnerability.

9.8 **CVE-2025-63807** 2dogz blogin

An issue was discovered in weijiang1994 university-bbs (aka Blogin) in commit 9e06bab430bfc729f27b4284ba7570db3b11ce84 (2025-01-13). A weak verification code generation mechanism combined with missing rate limiting allows attackers to perform brute-force attac

9.8 **CVE-2025-63685** Quark quark cloud drive

Quark Cloud Drive v3.23.2 has a DLL Hijacking vulnerability. This vulnerability stems from the insecure loading of system libraries. Specifically, the application does not validate the path or signature of [regsvr32.exe] it loads. An attacker can place a craft

9.2 **CVE-2025-12414**

An attacker could take over a Looker account in a Looker instance configured with OIDC authentication, due to email address string normalization.Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted.

9.6 **CVE-2025-10571**

Authentication Bypass Using an Alternate Path or Channel vulnerability in ABB ABB Ability Edgenius.This issue affects ABB Ability Edgenius: 3.2.0.0, 3.2.1.1.

9.8 **CVE-2025-52410** Vishalmathur institute-of-current-students

Institute-of-Current-Students v1.0 contains a time-based blind SQL injection vulnerability in the mydetailsstudent.php endpoint. The `myds` GET parameter is not adequately sanitized before being used in SQL queries.

Ransomware

No leak-site posts collected.

New data breaches 4

Beckett Collectibles beckett.com	1,041,238 accounts
International Kiteboarding Organization ikointl.com	340,349 accounts
Vultr vultr.com	187,872 accounts
Eurofiber eurofiber.com	10,003 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.