Daily brief, Wednesday, April 15, 2026

Apr 14, 8:00 PM to Apr 15, 8:00 PM ET

Generated Nov 7, 2026, 7:01 AM ET

0	0	0	18	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

18 new critical CVEs.

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

18

9.9 **CVE-2026-20147** Cisco identity services engine passive identity connector

A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative cred

9.9 **CVE-2026-20180** Cisco identity services engine

+1 more CVEs in the same release

A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read On

9.6 **CVE-2026-6296** Google chrome

Heap buffer overflow in ANGLE in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.9 **CVE-2026-39842** Openremote openremote

OpenRemote is an open-source IoT platform. Versions 1.21.0 and below contain two interrelated expression injection vulnerabilities in the rules engine that allow arbitrary code execution on the server. The JavaScript rules engine executes user-supplied scripts

9.8 **CVE-2026-1555**

The WebStack theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the io_img_upload() function in all versions up to, and including, 1.2024. This makes it possible for unauthenticated attackers to upload arbitrary

9.8 **CVE-2026-3461**

The Visa Acceptance Solutions plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.1.0. This is due to the `express_pay_product_page_pay_for_order()` function logging users in based solely on a user-supplied billi

9.8 **CVE-2026-30625**

Upsonic 0.71.6 contains a remote code execution vulnerability in its MCP server/task creation functionality. The application allows users to define MCP tasks with arbitrary command and args values. Although an allowlist exists, certain allowed commands (npm, n

9.8 **CVE-2026-20184**

A vulnerability in the integration of single sign-on (SSO) with Control Hub in Cisco Webex Services could have allowed an unauthenticated, remote attacker to impersonate any user within the service. This vulnerability existed because of improper certificate va

9.8 **CVE-2026-30993**

Slah CMS v1.5.0 and below was discovered to contain a remote code execution (RCE) vulnerability in the session() function at config.php. This vulnerability is exploitable via a crafted input.

9.8 **CVE-2026-5189** Sonatype nexus repository manager

CWE-798: Use of Hard-coded Credentials in Sonatype Nexus Repository Manager versions 3.0.0 through 3.70.5 allows an unauthenticated attacker with network access to gain unauthorized read/write access to the internal database and execute arbitrary OS commands a

9.4 **CVE-2026-40173** Dgraph dgraph

Dgraph is an open source distributed GraphQL database. Versions 25.3.1 and prior contain an unauthenticated credential disclosure vulnerability where the /debug/pprof/cmdline endpoint is registered on the default mux and reachable without authentication, expos

9.3 **CVE-2026-5387**

The vulnerability, if exploited, could allow an unauthenticated miscreant to perform operations intended only for Simulator Instructor or Simulator Developer (Administrator) roles, resulting in privilege escalation with potential for modification of simulation

9.3 **CVE-2025-15610**

The .NET Remoting framework used by OpenText Fax (RightFax) includes known security vulnerabilities that could be exploited if the service is exposed in environments where the remoting ports are accessible.

9.1 **CVE-2026-33807** Fastify fastify\/express

@fastify/express v4.0.4 and earlier contains a path handling bug in the onRegister function that causes middleware paths to be doubled when inherited by child plugins. When a child plugin is registered with a prefix that matches a middleware path, the middlewa

9.1 **CVE-2026-33808** Fastify fastify\/express

Impact@fastify/express v4.0.4 and earlier fails to normalize URLs before passing them to Express middleware when Fastify router normalization options are enabled. This allows complete bypass of path-scoped authentication middleware via duplicate slashes when i

9.1 **CVE-2025-41118** Grafana pyroscope

Pyroscope is an open-source continuous profiling database. The database supports various storage backends, including Tencent Cloud Object Storage (COS). If the database is configured to use Tencent COS as the storage backend, an attacker could extract the secr

9.1 **CVE-2026-6388**

A flaw was found in ArgoCD Image Updater. This vulnerability allows an attacker, with permissions to create or modify an ImageUpdater resource in a multi-tenant environment, to bypass namespace boundaries. By exploiting insufficient validation, the attacker ca

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

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.