Daily brief, Friday, April 17, 2026

Apr 16, 8:00 PM to Apr 17, 8:00 PM ET

Generated Nov 7, 2026, 6:41 AM ET

0	0	0	17	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

17 new critical CVEs, 1 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

17

9.9 **CVE-2026-40342** Firebirdsql firebird

Firebird is an open-source relational database management system. In versions prior to 5.0.4, 4.0.7 and 3.0.14, the external engine plugin loader concatenates a user-supplied engine name into a filesystem path without filtering path separators or .. components

9.8 **CVE-2026-34018** Cubecart cubecart

An SQL injection vulnerability exists in CubeCart prior to 6.6.0, which may allow an attacker to execute an arbitrary SQL statement on the product.

9.8 **CVE-2026-6443**

All plugins by Essentialplugin for WordPress are vulnerable to an injected backdoor in various versions. This is due to the plugin being sold to a malicious threat actor that embedded a backdoor in all of the plugin's they acquired. This makes it possible for

9.8 **CVE-2025-15625** Sparxsystems pro cloud server

Unauthenticated user is able to execute arbitrary SQL commands in Sparx Pro Cloud Server database in certain cases.

9.8 **CVE-2026-37749**

A SQL injection vulnerability in CodeAstro Simple Attendance Management System v1.0 allows remote unauthenticated attackers to bypass authentication via the username parameter in index.php.

9.8 **CVE-2026-35546** Anviz cx7 firmware

Anviz CX2 Lite and CX7 are vulnerable to unauthenticated firmware uploads. This causes crafted archives to be accepted, enabling attackers to plant and execute code and obtain a reverse shell.

9.8 **CVE-2026-29013** Libcoap libcoap

libcoap contains out-of-bounds read vulnerabilities in OSCORE Appendix B.2 CBOR unwrap handling where get_byte_inc() in src/oscore/oscore_cbor.c relies solely on assert() for bounds checking, which is removed in release builds compiled with NDEBUG. Attackers c

9.8 **CVE-2026-40351** Fastgpt fastgpt

FastGPT is an AI Agent building platform. In versions prior to 4.14.9.5, the password-based login endpoint uses TypeScript type assertion without runtime validation, allowing an unauthenticated attacker to pass a MongoDB query operator object (e.g., {"$ne": ""

9.1 **CVE-2026-6284**

An attacker with network access to the PLC is able to brute force discover passwords to gain unauthorized access to systems and services. The limited password complexity and no password input limiters makes brute force password enumeration possible.

9.1 **CVE-2026-40525** Volcengine openviking

OpenViking prior to version 0.3.9 contains an authentication bypass vulnerability in the VikingBot OpenAPI HTTP route surface where the authentication check fails open when the api_key configuration value is unset or empty. Remote attackers with network access

9.1 **CVE-2026-33516** Neutrinolabs xrdp

xrdp is an open source RDP server. Versions through 0.10.5 contain an out-of-bounds read vulnerability during the RDP capability exchange phase. The issue occurs when memory is accessed before validating the remaining buffer length. A remote, unauthenticated a

9.1 **CVE-2026-23500** Dolibarr dolibarr erp\/crm

Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. In versions prior to 23.0.0 , the ODT to PDF conversion process in odf.php concatenates the MAIN_ODT_AS_PDF configuration constant directly into a sh

9.1 **CVE-2026-33689** Neutrinolabs xrdp

xrdp is an open source RDP server. Versions through 0.10.5 have an out-of-bounds read vulnerability in the pre-authentication RDP message parsing logic. A remote, unauthenticated attacker can trigger this flaw by sending a specially crafted sequence of packets

9.1 **CVE-2026-40258**

The Gramps Web API is a Python REST API for the genealogical research software Gramps. Versions 1.6.0 through 3.11.0 have a path traversal vulnerability (Zip Slip) in the media archive import feature. An authenticated user with owner-level privileges can craft

9.1 **CVE-2026-5720** Miniupnp Project miniupnpd

miniupnpd contains an integer underflow vulnerability in SOAPAction header parsing that allows remote attackers to cause a denial of service or information disclosure by sending a malformed SOAPAction header with a single quote. Attackers can trigger an out-of

9.0 **CVE-2026-40477** Thymeleaf thymeleaf

+1 more CVEs in the same release

Thymeleaf is a server-side Java template engine for web and standalone environments. Versions 3.1.3.RELEASE and prior contain a security bypass vulnerability in the expression execution mechanisms. Although the library provides mechanisms to prevent expression

Ransomware

No leak-site posts collected.

New data breaches 1

Amtrak amtrak.com 2,147,679 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.