Daily brief, Wednesday, July 22, 2026

Jul 21, 8:00 PM to Jul 22, 8:00 PM ET

Generated Nov 3, 2026, 11:00 AM ET

0	2	0	20	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 20 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

9.8 **CVE-2026-50522** Microsoft SharePoint CISA KEV

An attacker gains remote code execution on Microsoft SharePoint without authentication.

9.3 **CVE-2026-16232** Check Point SmartConsole CISA KEV DETECTION

An unauthenticated remote attacker can obtain an application login token and use it to authenticate with full administrative privileges on Check Point SmartConsole.

New public exploit code

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

New critical CVEs 20

9.3 **CVE-2026-16232** Check Point SmartConsole KEV EXPLOIT CODE DETECTION

An unauthenticated remote attacker can obtain an application login token and use it to authenticate with full administrative privileges on Check Point SmartConsole.

9.8 **CVE-2026-50522** Microsoft SharePoint KEV EXPLOIT CODE

An attacker gains remote code execution on Microsoft SharePoint without authentication.

10.0 **CVE-2026-60366** Oracle platform security for java

+3 more CVEs in the same release

Vulnerability in the Oracle Platform Security for Java product of Oracle Fusion Middleware (component: Centralized Thirdparty Jars). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated att

9.8 **CVE-2026-65590** N8n n8n

n8n before 2.29.8 and 2.30.x before 2.30.1 does not enforce shell sandbox restrictions on Linux and Windows in the @n8n/computer-use package (sandboxing was applied only on macOS). Shell commands executed by the tool run without any filesystem or network restr

9.8 **CVE-2026-2395**

Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Xpoda Türkiye Informatics Technology Inc. No Code Platform allows SQL Injection. This issue affects No Code Platform: from 4.1.3 before 4.1.4.

9.8 **CVE-2026-16606**

A vulnerability in Fujitsu Software Linux openFT and Fujitsu Software Oracle Solaris openFT before version 12.1D00 allows for unauthenticated remote code execution (pre-auth RCE) on GNU/Linux or Oracle Solaris. The Fsas Technologies PSIRT obtained that intelli

9.8 **CVE-2025-50329**

An issue in ConeXware, Inc Power Archiver v.22.00.11 and before allows a remote attacker to escalate privileges and execute arbitrary code via the powerarc.exe.

9.8 **CVE-2026-64796**

Joomla Extension - regularlabs.com - various code injection vectors in Sourcerer extension - Free did not require both the article creator and last modifier to be Super Users before executing article PHP. Pro did not consistently enforce configured CSS, JavaSc

9.6 **CVE-2026-16624**

Cal.com OSS ships lacks authorization on webhook teamId creation, allowing any authenticated user to create a webhook on any team via unvalidated teamId injection, then steal booking data, including fields like organizer/attendee emails and custom responses, a

9.4 **CVE-2026-63048**

Joomla Extension - joomlack.fr - Improper access control in Page Builder CK 1.0.0-3.1.2, 3.4.0-3.4.11, 3.5.0-3.6.2 - The Joomla extension Page Builder CK is vulnerable to an authenticated arbitrary file upload, leading to RCE.

9.3 **CVE-2026-8152**

Unblu Spark contains an open redirect vulnerability that can be escalated to a DOM-based cross-site scripting (XSS) attack. When Unblu Spark is deployed with com.unblu.identifier.siteEmbeddedSetup=true, it runs in the same origin as the host application. Any J

9.3 **CVE-2026-50252** Nlnetlabs unbound

In NLnet Labs Unbound 1.4.22 up to and including 1.25.1, UDP source port is randomized and intended to serve as a secret value that increases the entropy of DNS transactions. When resolver load balancing policies depend on the source port while their outcome i

9.1 **CVE-2026-62144**

An authentication bypass vulnerability in Check Point Security Management and Multi-Domain Security Management allows an unauthenticated remote attacker to execute administrative commands on the Management Server. Successful exploitation may also allow command

9.1 **CVE-2026-40712** Dell powerprotect data manager

+1 more CVEs in the same release

Dell PowerProtect Data Manager, versions prior to 20.2.0.0, contain(s) an Improper Input Validation vulnerability in the REST API. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.

9.1 **CVE-2026-64793**

Joomla Extension - regularlabs.com - Content access and publication bypass in Articles Anywhere and Modules Anywhere extensions - Content tags could use ignore flags or property overrides to render restricted or unpublished articles or modules. A content autho

9.1 **CVE-2026-64798**

Joomla Extension - regularlabs.com - Insecure login URL keys in IP login extension - Persistent URL login keys were also generated using a non-cryptographic random generator with insufficient entropy.

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. CVE IDs link to the full record on Watch Floor.