Daily brief, Monday, June 15, 2026

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

Generated Nov 4, 2026, 10:23 PM ET

0	2	0	80	0	3
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 80 new critical CVEs, 3 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.5 **CVE-2026-54420** LiteSpeed cPanel Plugin CISA KEV

LiteSpeed cPanel plugin contains a UNIX symbolic link (Symlink) following vulnerability that could allow a user with FTP or web shell access on a shared hosting server running CloudLinux/CageFS.

6.5 **CVE-2026-20262** Cisco Catalyst SD-WAN Manager CISA KEV

An authenticated attacker can create a file or overwrite any file on the filesystem of Cisco Catalyst SD-WAN Manager.

New public exploit code

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

New critical CVEs

80

10.0 **CVE-2026-52704**

Improper Control of Generation of Code ('Code Injection') vulnerability in Edgar Rojas WooCommerce PDF Invoice Builder allows Remote Code Inclusion. This issue affects WooCommerce PDF Invoice Builder: from n/a through 2.0.8.

10.0 **CVE-2026-40772**

Unauthenticated Arbitrary File Upload in GeekyBot <= 1.2.2 versions.

10.0 **CVE-2026-48836**

Unauthenticated Remote Code Execution (RCE) in Easy Invoice <= 2.1.19 versions.

9.9 **CVE-2026-39591**

Subscriber Arbitrary File Upload in WP-BusinessDirectory <= 4.0.0 versions.

9.9 **CVE-2026-49766**
Subscriber Arbitrary File Deletion in WP User Manager <= 2.9.16 versions.

9.8 **CVE-2026-8935**
The WP MAPS PRO WordPress plugin before 6.1.1 registers an unauthenticated AJAX action which, given a valid nonce that is publicly emitted on any frontend page enqueuing its map script, unconditionally creates an administrator account and returns a magic-login

9.8 **CVE-2018-25436**
WordPress Plugin Baggage Freight Shipping Australia 0.1.0 contains an unrestricted file upload vulnerability that allows unauthenticated attackers to upload arbitrary files by exploiting the upload-package.php endpoint. Attackers can submit POST requests with

9.8 **CVE-2026-9862** Fortra core privileged access manager server
Fortra's Core Privileged Access Manager (BoKS) contains an OS command injection vulnerability in the boks_autoregisterd service. A remote attacker with network access to the service may be able to cause commands to be executed with the privileges of the servic

9.8 **CVE-2026-30120** Remotion remotion
remotion-dev remotion v4.0.409 was discovered to contain a remote code execution (RCE) vulnerability.

9.8 **CVE-2026-36537**
ThingsBoard v4.3.0.1 is vulnerable to an authentication bypass during the OAuth authorization code exchange. The application improperly trusts user-supplied identity data within the user parameter of the /login/oauth2/code/ endpoint. By manipulating the email

9.8 **CVE-2026-38060**
Tenda 5G03 V05.03.02.04 (Version 1.0) is vulnerable to Command injection in the function action_unlock_sim via the pin parameter.

9.8 **CVE-2026-38061**
Tenda 5G03 V05.03.02.04 (Version 1.0) is vulnerable to Command injection in the function action_set_volume via the volume parameter.

9.8 **CVE-2026-38062**
Tenda 5G03 V05.03.02.04 (Version 1.0) is vulnerable to Command injection in the function action_set_rat_mode via the ratMode parameter.

9.8 **CVE-2026-38063**
Tenda 5G03 V05.03.02.04 (Version 1.0) is vulnerable to Command injection in the function action_radio_on_with_ia_apn via the ia parameter.

9.8 **CVE-2026-38064**
Tenda 5G03 V05.03.02.04 (Version 1.0) is vulnerable to Command injection in the function action_dial_call via the dialNumber parameter.

9.8 **CVE-2026-38065**
Tenda 5G03 V05.03.02.04 (Version 1.0) is vulnerable to Command injection in the function action_ims_on_with_apn via the ims_apn parameter.

9.8 **CVE-2026-38329**

Bludit CMS before version 3.18.4 allows Remote Code Execution (RCE) via the API Plugin. The POST /api/files/{key} endpoint in bl-plugins/api/plugin.php fails to perform authorization checks and lacks file extension validation. An attacker with a valid API toke

9.8 **CVE-2026-38812**

RuoYi v4.8.2 is vulnerable to SQL Injection via the /tool/gen/createTable endpoint. The issue affects the code generation module and may allow an authenticated attacker with administrative privileges to access sensitive database information.

9.8 **CVE-2026-39006**

An issue in SNMP4J-Agent 3.8.3 allows a remote attacker to execute arbitrary code via the snmp4jCfgStoragePath component.

9.8 **CVE-2026-39196**

Datadog, Inc Vector v0.54.0 was discovered to contain a SQL injection vulnerability in the set_uri_query parameter in the KeyPartitioner::partition function. This vulnerability allows attackers to access sensitive database information via crafted SQL statement

60 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 3

June 2026 Stealer Logs	56,278,397 accounts
Berkadia berkadia.com	305,216 accounts
Infinite Campus infinitecampus.com	137,123 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. CVE IDs link to the full record on Watch Floor.