# Daily brief, Thursday, July 16, 2026

Jul 15, 8:00 PM to Jul 16, 8:00 PM ET

Generated Nov 3, 2026, 4:36 PM ET

| 0 | 3 | 0 | 36 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

3 newly exploited, 36 new critical CVEs.

## Breaking

*Nothing spreading fast in technology large companies run.*

## Newly exploited in the wild 3

**9.8** **CVE-2026-58644** Microsoft SharePoint CISA KEV DETECTION

An attacker gains remote code execution with Microsoft SharePoint.

**9.1** **CVE-2026-39808** Fortinet FortiSandbox CISA KEV DETECTION

An attacker gains arbitrary system command execution and remote code execution on the Fortinet FortiSandbox appliance.

**9.1** **CVE-2026-25089** Fortinet FortiSandbox CISA KEV

An attacker gains remote code execution and full control of the Fortinet FortiSandbox appliance.

## New public exploit code

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

## New critical CVEs 36

**9.1** **CVE-2026-39808** Fortinet FortiSandbox KEV EXPLOIT CODE DETECTION

**+1 more CVEs in the same release**

An attacker gains arbitrary system command execution and remote code execution on the Fortinet FortiSandbox appliance.

**9.8** **CVE-2026-58644** Microsoft SharePoint KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution with Microsoft SharePoint.

9.8 **CVE-2026-53412** Zoom workplace desktop

Improper Input Validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an account takeover via network access.

9.3 **CVE-2026-59865** Microsoft kiota

Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.29.1 and 1.32.5, `kiota info` read x-ms-kiota-info.languagesInformation.<language>.dependencyInstallCommand plus dependency name and version values from an OpenAPI description and presented the s

9.3 **CVE-2026-59866** Microsoft kiota

Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.29.1 and 1.32.5, Kiota emitted x-ms-kiota-info clientClassName and clientNamespaceName values without identifier or path sanitization as both generated client class or namespace names and generat

9.3 **CVE-2026-59864** Microsoft kiota

Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.29.1 and 1.32.5, `kiota plugin add` and `kiota plugin generate` (with `-t APIPlugin`) emitted attacker-controlled static_template.file values from x-ai-adaptive-card and x-ai-capabilities into ge

9.3 **CVE-2026-54733** Microsoft o365-moodle

The Microsoft 365 and Microsoft Entra ID Plugins for Moodle provide Office 365 and Azure Active Directory integration for Moodle. Prior to 4.5.6, 5.0.5, and 5.1.1, the Microsoft Office 365 Integration plugin local_o365 Teams SSO endpoint sso_login.php base64-d

9.8 **CVE-2026-63087** Grafana-Cold-Storage oncall

Grafana OnCall through 1.16.11 contains an unauthenticated access vulnerability that allows remote attackers to obtain a valid PluginAuthToken by sending a POST request to the internal plugin install endpoint using hardcoded default stack_id and org_id values

9.8 **CVE-2026-3031** TOKUHIROM Image::EPEG

Image::EPEG versions through 0.15 for Perl embeds an unsupported version of the Epeg library. Image::EPEG includes Epeg 0.9.0 that was last updated in 2004. Epeg is a fast JPEG thumbnail library that was once part of the Englightenment Project.

9.1 **CVE-2026-57073** CODECHILD HTML::Bare

HTML::Bare versions through 0.04 for Perl have an unbounded character lookahead. The parserc_parse function attempts to check for multicharacter strings such as "<![CDATA" or element terminators such as ">" without checking that the offsets are within the buff

9.9 **CVE-2026-46512** Mwtcmi frogman

Frogman provides headless PBX control through MCP and HTTP API. Prior to 1.6.2, fm_dialplan_apply accepted template parameters including greeting, dest, url, extension, code, and file, and Tools/DialplanApply.php wrote Dialplan/Templates.php output to extensio

9.1 **CVE-2026-57074** CODECHILD XML::Bare

XML::Bare versions through 0.53 for Perl have an unbounded character lookahead. The parserc_parse function attempts to check for multicharacter strings such as "<![CDATA" or element terminators such as ">" without checking that the offsets are within the buffe

**10.0** **CVE-2026-45336** StratonWebDesigners HireFlow

HireFlow is a web-based interview management system for managing candidates, scheduling interviews, and tracking hiring progress. In 1.2 and earlier, app.py assigns a hard-coded Flask secret_key used to sign session cookies, allowing unauthenticated attackers

**9.1** **CVE-2026-45568** Netfoundry zrok

zrok is software for sharing web services, files, and network resources. Prior to 2.0.3, zrok's Python SDK ProxyShare Flask proxy route accepts an absolute URL in the request path and passes it to urllib.parse.urljoin, allowing the requested path to replace th

**10.0** **CVE-2026-44181** Jupyter enterprise gateway

**+2 more CVEs in the same release**

Jupyter Enterprise Gateway launches remote Jupyter Notebook kernels across distributed clusters like Apache Spark, Kubernetes, and Docker Swarm. In versions 2.0.0rc2 and above, prior to 3.3.0, the environment variables (KERNEL_XXX) used during the rendering of

**9.9** **CVE-2026-54526** Argoproj argo workflows

Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Prior to 3.7.15 and 4.0.6, the allow-list fix for CVE-2026-31892 is incomplete because workflow/util/merge.go ValidateUserOverrides and SanitizeUse

**9.8** **CVE-2026-15013**

The SAML Single Sign On – SSO Login plugin for WordPress is vulnerable to Authentication Bypass via SAML Signature Algorithm Confusion in all versions up to, and including, 5.4.3. The vulnerability exists because `Mo_SAML_Utilities::mo_saml_cast_key()` reads t

**9.8** **CVE-2026-12492**

The Happy Coders OTP Login for WooCommerce WordPress plugin before 2.8 does not verify that a one-time password was actually validated before authenticating a user based on a supplied identifier, allowing unauthenticated attackers to log in as any existing use

**9.8** **CVE-2023-49899**

An unauthenticated remote attacker can execute any command on the affected device due to not correctly verifying the origin of a communication channel.

**9.8** **CVE-2023-49900**

An unauthenticated remote attacker is able to perform remote code execution due to incorrectly sanitized user input in the SetParameter command.

*13 more critical CVEs in this window: see the dashboard*

## 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.