Daily brief, Friday, March 13, 2026

Mar 12, 8:00 PM to Mar 13, 8:00 PM ET

Generated Nov 7, 2026, 1:16 PM ET

0	2	0	14	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 14 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.8 **CVE-2026-3909** Google Skia CISA KEV

An out-of-bounds write in Google Skia lets a remote attacker access memory out of bounds via a crafted HTML page, affecting Chrome, ChromeOS, Android, and Flutter.

8.8 **CVE-2026-3910** Google Chromium V8 CISA KEV

A remote attacker gets arbitrary code execution inside the sandbox via a crafted HTML page in Google Chromium V8, affecting browsers built on Chromium.

New public exploit code

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

New critical CVEs

14

9.8 **CVE-2026-32746** GNU inetutils EXPLOIT CODE DETECTION

Product not on watchlist.

9.8 **CVE-2026-3891** DETECTION

The Pix for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check and missing file type validation in the 'lkn_pix_for_woocommerce_c6_save_settings' function in all versions up to, and including, 1.5.0. This m

9.8 **CVE-2026-1668** Tp-Link omada sg2005p-pd firmware

The web interface on multiple Omada switches does not adequately validate certain external inputs, which may lead to out-of-bound memory access when processing crafted requests. Under specific conditions, this flaw may result in unintended command execution.<b

9.8 **CVE-2026-25823**

+1 more CVEs in the same release

HMS Networks Ewon Flexy with firmware before 15.0s4, Cosy+ with firmware 22.xx before 22.1s6, and Cosy+ with firmware 23.xx before 23.0s3 have a stack buffer overflow that leads to a Denial of Service, which can also be exploited to achieve Unauthenticated Rem

9.8 **CVE-2026-31806** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.24.0, the gdi_surface_bits() function processes SURFACE_BITS_COMMAND messages sent by the RDP server. When the command is handled using NSCodec, the bmp.width and bmp.height values pro

9.9 **CVE-2026-32306** Hackerbay oneuptime

OneUptime is a solution for monitoring and managing online services. Prior to 10.0.23, the telemetry aggregation API accepts user-controlled aggregationType, aggregateColumnName, and aggregationTimestampColumnName parameters and interpolates them directly into

9.8 **CVE-2026-32304** Locutus locutus

Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. Prior to 3.0.14, the create_function(args, code) function passes both parameters directly to the Function constructor without any sanitization, allowing arbitrary cod

10.0 **CVE-2026-26954** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.34, it is possible to obtain arrays containing Function, which allows escaping the sandbox. Given an array containing Function, and Object.fromEntries, it is possible to construct {[p]: Function} where

9.4 **CVE-2026-23941** Erlang erlang\Vinets

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in Erlang OTP (inets httpd module) allows HTTP Request Smuggling. This vulnerability is associated with program files lib/inets/src/http_server/httpd_request.erl and program

9.1 **CVE-2026-31886** Dagu dagu

Dagu is a workflow engine with a built-in Web user interface. Prior to 2.2.4, the dagRunId request field accepted by the inline DAG execution endpoints is passed directly into filepath.Join to construct a temporary directory path without any format validation.

9.1 **CVE-2026-32367**

Improper Control of Generation of Code ('Code Injection') vulnerability in Yannick Lefebvre Modal Dialog modal-dialog allows Remote Code Inclusion.This issue affects Modal Dialog: from n/a through <= 3.5.16.

9.9 **CVE-2026-22192** Gvectors wpdiscuz

Voltronic Power SNMP Web Pro version 1.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to access privileged management functions by manipulating browser localStorage values. Attackers can modify client-side authenticatio

9.3 **CVE-2026-32301** Centrifugal centrifugo

Centrifugo is an open-source scalable real-time messaging server. Prior to 6.7.0, Centrifugo is vulnerable to Server-Side Request Forgery (SSRF) when configured with a dynamic JWKS endpoint URL using template variables (e.g. {{tenant}}). An unauthenticated att

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.