Google Chrome Multiple High-Severity Vulnerabilities

Severity Level: High

Components Affected

- Google Chrome Stable for desktop installations not yet updated to the fixed builds: **150.0.7871.186/.187 for Windows and macOS, and 150.0.7871.186 for Linux**.

Overview

On 23 July 2026, Google released a Stable Channel update for Google Chrome on desktop that addresses four High-severity security vulnerabilities. The issues are tracked as CVE-2026-16804, CVE-2026-16805, CVE-2026-16806, and CVE-2026-16807, and comprise three use-after-free flaws and one out-of-bounds write flaw. Organizations and users should update affected Chrome installations promptly.

Description

Google updated the Chrome Stable Channel to versions 150.0.7871.186/.187 for Windows and macOS and 150.0.7871.186 for Linux. The release contains four security fixes: CVE-2026-16807 (out-of-bounds write in Codecs), CVE-2026-16806 (use-after-free in WebMCP), CVE-2026-16805 (use-after-free in Blink), and CVE-2026-16804 (use-after-free in Input).

The CVE records state that CVE-2026-16805 and CVE-2026-16806 can allow a remote attacker to execute arbitrary code inside the Chrome sandbox through a crafted HTML page. CVE-2026-16807 can potentially enable a sandbox escape through a crafted HTML page, while CVE-2026-16804 can potentially enable a sandbox escape after the renderer process has been compromised.

Google has restricted access to detailed bug information until a majority of users have received the fixes. The vendor release note does not state that these four vulnerabilities are under active exploitation. Defensive action should therefore focus on rapid patching and confirmation that the updated browser has been restarted and is running the fixed build.

Impact

- Arbitrary code execution inside the Chrome sandbox (CVE-2026-16805 and CVE-2026-16806)
- Potential Chrome sandbox escape (CVE-2026-16804 and CVE-2026-16807)
- Potential compromise of the confidentiality, integrity, and availability of the affected endpoint if exploitation succeeds

Solution/ Workarounds

Before deployment, review the vendor advisory and test the update in accordance with the organization's change-management procedures.

Apply the latest Google Chrome Stable security update:

- Update Chrome to **150.0.7871.186/.187 or later on Windows and macOS, and 150.0.7871.186 or later on Linux**.
- Restart Chrome after updating and verify the installed version from Menu > Help > About Google Chrome.
- Enable automatic browser updates and monitor managed endpoints for failed or pending updates.
- Prioritize devices used to browse untrusted internet content or access sensitive organizational systems.

Reference

- Google Chrome Stable Channel Update for Desktop - 23 July 2026
  NVD: CVE-2026-16804, CVE-2026-16805, CVE-2026-16806, CVE-2026-16807; CERT-FR Advisory CERTFR-2026-AVI-0925

Disclaimer

The information provided herein is based on public vendor and government sources available as of 28 July 2026 and is provided on an "as is" basis, without warranty of any kind.