contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Google Chromium exploited

CVE-2026-125350 · on CISA's exploited list since 10 November 2026

Analysis Report

Anyone running Google Chrome below 157.0.8103.50 must update before 24 November 2026; CISA has listed this as exploited. Check the installed Chrome version first — if it is below 157.0.8103.50 ...

PREPARED BY	NamiQ	DATE	11 November 2026
FACTS AS OF	11 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.8**	STATUS	On CISA's exploited list; due 24 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/google-chromium-cve-2026-125350

The bottom line

> *Anyone running Google Chrome below 157.0.8103.50 must update before 24 November 2026; CISA has listed this as exploited. Check the installed Chrome version first — if it is below 157.0.8103.50, update now.*

At a glance

Fact	Detail
Product	Google Chromium (CVE-2026-125350)
Severity	High: 8.8 (CVSS 3.1)
CISA	On its exploited list since 10 November 2026. Deadline for US federal agencies: 24 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 11 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Google Chrome 157.0.8103.50. The record description states versions prior to this are affected. No source names a fixed version for Microsoft Edge or Opera.
Who looks first	Anyone running Google Chrome, Microsoft Edge, Opera, or another Chromium-based browser. CISA says the flaw could affect any browser built on Chromium. IT teams managing fleets where browser auto-update is disabled or controlled by policy need to act first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you use Google Chrome, Microsoft Edge, Opera, or another Chromium-based browser?	Nothing to do for this CVE.	Check the installed version.
Is your Chrome version below 157.0.8103.50?	Chrome is patched; check Edge and Opera separately if used.	Update Chrome to 157.0.8103.50 or later immediately.

Do you also run Microsoft Edge or Opera?	Nothing further for Chromium-based browsers.	No fixed version is named in the record for those; seek guidance from those vendors.

What it is

A use-after-free flaw in Chromium's XML component lets a remote attacker run arbitrary code inside the browser sandbox. The only thing needed is for a user to visit a specially crafted webpage; no login or file download is required.

Why it matters

A use-after-free means the browser accesses memory it has already freed, letting an attacker corrupt execution state through crafted XML content. The record scores this 8.8 and places execution inside the browser sandbox. Our reading is that sandboxed code execution is still a meaningful foothold: it is typically the first stage before a sandbox-escape attempt, and CISA's listing signals confirmed exploitation rather than theoretical risk. The low EPSS of 0.00962 may reflect how recently this was listed rather than its real-world spread.

Things people will get wrong

- Auto-update means Chrome is already protected. Auto-update can be delayed or suppressed by group policy in managed environments. Confirm the installed version is 157.0.8103.50 or later before closing the ticket.
- This only affects Google Chrome, not Edge or Opera. CISA says the flaw could affect any browser using Chromium, including Microsoft Edge and Opera. The record names only Chrome's fixed version; those vendors must be consulted separately.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Identify all Chromium-based browsers in use

- List every installed browser across managed endpoints — Google Chrome, Microsoft Edge, Opera, and any other Chromium-based product.
- Record the installed version of each before proceeding.

```
google-chrome --version
microsoft-edge --version
```

Step 2: Check Chrome against the fixed version

- The record description states Chrome prior to 157.0.8103.50 is affected. Any instance below that version needs updating.
- If update policy is managed centrally, push the update rather than waiting for the next scheduled cycle.

Step 3: Update Chrome to 157.0.8103.50 or later

- Apply the update through your patch management process or via the browser itself (menu → Help → About Google Chrome).
- CISA's deadline is 24 November 2026.

Step 4: Seek guidance for Edge and Opera

- The record names no fixed version for Edge or Opera. Consult those vendors' security advisories for their guidance.
- Until a fix is confirmed, consider whether those browsers need to remain in use on externally exposed systems.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We need to act on CVE-2026-125350, a use-after-free in Chromium's XML component that allows remote code execution inside the browser sandbox via a crafted webpage. CISA requires action by 24 November 2026. The record states Chrome prior to version 157.0.8103.50 is affected; that version is the fix. The flaw may also affect Microsoft Edge and Opera, but no fixed version is named for them in the record. Please confirm: which Chromium-based browsers are deployed and their current versions; that Chrome has been updated to 157.0.8103.50 or later; and your guidance for Edge and Opera if deployed. We need written confirmation of installed versions and the fix by 22 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected browser crashes or crash reports referencing XML parsing, particularly after a user visited an unfamiliar site.
- Unusual child processes spawned by the browser, or network connections from browser processes to unexpected external hosts.
- New or modified files in browser profile directories or temporary folders around the time potentially malicious pages were visited.

The weakness behind it

The record classes this as CWE-416 (Use After Free).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Drive-by Compromise (T1189): Getting a visitor's browser to run harmful content from a website.	Initial Access: getting in	The flaw triggers by visiting a crafted webpage with no user action beyond normal browsing — this would typically be a drive-by delivery pattern.
Exploitation for Client Execution (T1203): Making a program run the attacker's code by exploiting a flaw in software a person opens.	Execution: running the attacker's code	The browser is the client being exploited; the record says arbitrary code executes inside it via a crafted HTML page, which is client-side exploitation.
Escape to Host (T1611): Breaking out of a container to reach the machine that hosts it.	Privilege Escalation: gaining higher rights	Sandboxed execution would likely be used as a first stage toward escaping the browser sandbox, though the record does not state that has occurred.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Google Chromium contains a use-after-free vulnerability in the XML component that could allow a remote attacker to execute arbitrary code inside the sandbox via a specially crafted webpage. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.*

The CVE record, published by Chrome on 10 November 2026:

> *Use after free in XML in Google Chrome prior to 157.0.8103.50 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)*

Versions of Google Chrome the record lists as affected:

- 157.0.8103.50 up to, but not including, 157.0.8103.50

The affected ranges end before 157.0.8103.50. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-125350
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel

version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-125350
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- Whether the sandboxed execution this flaw enables has been paired with a sandbox-escape in observed attacks.
- Fixed versions for Microsoft Edge and Opera; the record names only Chrome's fix.
- The specific XML feature or document structure that triggers the fault.
- Whether the Chrome Releases blog post of 9 November 2026 addresses this CVE specifically; the retrieved source text contains no advisory detail.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 11 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-125350: score 8.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	Required	A person must click, visit or open something.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
10 November 2026	CVE record published by Chrome.
10 November 2026	CISA added it to its list of exploited vulnerabilities.
24 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Chrome below 157.0.8103.50 deployed where auto-update is disabled or managed by group policy	High	Before 24 November 2026
Any Chromium-based browser used on systems that routinely browse external or untrusted websites	High	Before 24 November 2026
Microsoft Edge or Opera in use; the record names no fixed version for either	Medium	This week, pending vendor guidance

Chrome with auto-update active and no group policy restrictions in place	Low	Confirm version is at or above 157.0.8103.50

Appendix 4. Definition of done

- Every Google Chromium you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-125350: https://www.cve.org/CVERecord?id=CVE-2026-125350
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: chromereleases.googleblog.com/2026/11/stable-channel-update-for-desktop_01822: https://chromereleases.googleblog.com/2026/11/stable-channel-update-for-desktop_018223192.html
- Reference in the CVE record: issues.chromium.org: https://issues.chromium.org/issues/582442907