CVE-2026-125396

VULNERABILITY · CYBER DESK

Compiled by machine from news coverage; not reviewed analysis. A snapshot taken on 23 Nov 2026. Numbers in brackets point to the Sources list at the end. The live page: https://morningstarsecurity.com/wiki/cve-2026-125396

SUMMARY

Use-after-free in Ghostscript font loader allows sandbox escape and RCE via crafted PostScript/image files

FACTS

- **CVE:** CVE-2026-125396 (high confidence, 3 independent sources) [4]
- **CVSS:** 8.5 (medium confidence, 2 independent sources) [4]
- **KEV:** no (low confidence, 1 independent source) [3]
- **Weakness:** CWE-416: Use After Free (medium confidence, 2 independent sources) [4]
- **Disclosed:** 2026-11-15 (low confidence, 1 independent source) [4]
- **Patch status:** patch-available (high confidence, 3 independent sources) [4]

AFFECTED PRODUCT

- Ghostscript

ENTRY

Use-after-free in Ghostscript font loader allows sandbox escape and RCE via crafted PostScript/image files.

Drawn from 1 news source; the facts and relationships below show where each detail comes from.

CONNECTIONS

Links to other wiki entries, from the wiki's graph. This file gives no source for them: treat them as leads, not findings.

- **Affects:** Ghostscript

OFTEN MENTIONED TOGETHER

Entries that turn up in the same stories. This is not a stated relationship. Google, pwn.ai, GL.iNet, GoodCloud

ABOUT MORNINGSTAR SECURITY

MorningStar Security is a security news reader and community, started in 2009 and relaunched in 2026. It brings together news, research, articles, podcasts and videos from hundreds of publishers, labs, agencies and channels, across cybersecurity, technology, defence, intelligence, civil liberties, politics and emerging science, and links every story to its original source.

Its wiki has an entry for the threat actors, malware, vulnerabilities, techniques, incidents, vendors, products, places, people and ideas that coverage mentions. Each entry is compiled by machine from the stories the site indexes. Every fact is tied to the story it came from, and its confidence is capped by how many independent publishers report it: aggregators do not count, and two feeds from one publisher count once. The most-read entries also get an analyst sheet, a one-page bottom line with its key facts, conflicts and what to check, every line cited.

Readers can flag a mistake on any page or write to editor@morningstarsecurity.com.

- This entry, live: https://morningstarsecurity.com/wiki/cve-2026-125396
- More vulnerabilities (CVE): https://morningstarsecurity.com/wiki/kind/vulnerability
- The Cyber desk, for the news: https://morningstarsecurity.com/desk/cyber
- The whole wiki: https://morningstarsecurity.com/wiki
- About MorningStar Security: https://morningstarsecurity.com/about
- How the site is made: https://morningstarsecurity.com/editorial
- The newsletter: https://morningstarsecurity.com/newsletter

SOURCES

3. Proof-of-concept exploit code available for Ghostscript 'Upload2Shell' vulnerability (CVE-2026-125396) · Sophos News · 23 Nov 2026 · https://www.sophos.com/en-us/blog/proof-of-concept-available-for-ghostscript-upload2shell
4. Researchers Demonstrate Ghostscript Sandbox-Escape RCE via Crafted File Uploads in Popular Apps · The Hacker News · 22 Nov 2026 · https://thehackernews.com/2026/11/researchers-demonstrate-ghostscript.html

Not cited above. Other coverage that mentions CVE-2026-125396, for context only:

1. ⚡ Weekly Recap: VMware 0-Day, Java4Shell, NGINX2Root, Ruby2Shell, and a Whole Lot of Shell Trouble · The Hacker News · 23 Nov 2026 · https://thehackernews.com/2026/11/weekly-recap-vmware-0-day-java4shell.html

2. Syslog Timestamps; GL.iNet GoodCloud Breach; Ghostscript Upload2Shell RCE (CVE-2026-125396) (Nov 23rd 2026) · SANS ISC: Daily Podcast (podcast) · 23 Nov 2026 · https://isc.sans.edu/podcastdetail/10190

Snapshot of https://morningstarsecurity.com/wiki/cve-2026-125396 taken 23 Nov 2026 18:04 UTC. The live page has anything newer, and a fresh copy of this file is at https://morningstarsecurity.com/md/wiki/cve-2026-125396