

SECURITY ADVISORY

socfortress CoPilot: new CVE

CVE-2026-61738 · record published 30 October 2026

Analysis Report

If you run SOCFortress CoPilot below version 0.1.77, ask your IT provider this week to confirm the version and move to 0.1.77 or later. If you do not run CoPilot, you can stop reading.

PREPARED BY	NamiQ	DATE	31 October 2026
FACTS AS OF	31 October 2026	VERSION	1.0
SEVERITY	Critical: CVSS 3.1 10.0	STATUS	Not on CISA's exploited list; exploitation not recorded

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/socfortress-copilot-cve-2026-61738

The bottom line

If you run SOCFortress CoPilot below version 0.1.77, ask your IT provider this week to confirm the version and move to 0.1.77 or later. If you do not run CoPilot, you can stop reading.

At a glance

Fact	Detail
Product	socfortress CoPilot (CVE-2026-61738)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by GitHub on 30 October 2026. Not on CISA's list of exploited vulnerabilities when we read it on 31 October 2026, which means nothing public says yet that anyone is using it.
Fixed in	0.1.77, taken from the record's affected range (before 0.1.77). The sources give no release notes or fix date.
Who looks first	Anyone running SOCFortress CoPilot before 0.1.77, first those whose instance can be reached from the internet or by many staff. The record says admin and analyst users can reach the upload.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SOCFortress CoPilot?	Nothing to do for this CVE.	Check the version (next question).
Is your CoPilot version earlier than 0.1.77?	Not affected by this record. Keep the version note.	Check who can reach it (next question).
Can anyone outside a trusted network reach the CoPilot web interface or API?	Still patch, but within your normal cycle.	Restrict access now, then patch this week.

What it is

The Google Cloud report upload takes the file name from the request without cleaning it. A crafted name makes the server write the uploaded JSON outside the report folder, including into the application's own source folder, which can overwrite files on the host.

Why it matters

Our reading is that a file write outside the intended folder, in a backend the record says runs as root, is useful to an attacker for more than tampering with a report. Overwriting application files can change what the server runs. The record gives the score as 10 and says the written content must be valid Google Cloud report JSON, which limits what can be written but does not remove the risk.

Things people will get wrong

- "It is not on CISA's list, so nobody is using it." The record is new. Not being listed means CISA does not list it yet, not that nobody exploits it.
- "It needs an admin login, so we are safe." The description names admin and analyst users, but the score's own vector says no privileges are needed. The two disagree, so do not rely on the login.
- "It only writes a JSON file, so the damage is small." The record says the write lands outside the report folder, including the application source folder, in a backend running as root. That can overwrite host files.

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: Find the version you run

- Check whether CoPilot is installed and which version. The record treats anything before 0.1.77 as affected.
- Note where it runs and who can reach it.

```
docker ps --format '{{.Names}} {{.Image}}'  
docker images | grep -i copilot
```

Step 2: Reduce exposure

- Limit access to the CoPilot interface and API to trusted networks until it is patched.
- Review which admin and analyst accounts exist, since the record says they can reach the upload.

Step 3: Update to 0.1.77 or later

- Move to 0.1.77 or later, the version after the affected range in the record.
- Ask the vendor's release notes for any other changes in the same release.

Step 4: Check for signs of misuse

- Look for uploads to the Google Cloud report route with unusual file names, and for application files changed recently.

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.

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.

Hello, we need to know whether we run SOCFortress CoPilot, and if so where and which version. CVE-2026-61738 affects versions before 0.1.77 and allows files to be written outside the intended folder through the Google Cloud report upload. Please tell us whether any instance is exposed to the internet, update to 0.1.77 or later, and confirm the installed version and the fix to us in writing by the end of next week. Thank you.

The weakness behind it

The record classes this as CWE-22 and CWE-73 and CWE-434.

The sources, in their words

The CVE record:

SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.77, `POST /api/scoutsuite/generate-gcp-report` in `backend/app/integrations/scoutsuite/routes/scoutsuite.py` admits admin and analyst users and validates the uploaded content as `GCPScoutSuiteJSON`, but passes raw `file.filename` from the multipart header to `save_file_to_directory` in `backend/app/integrations/scoutsuite/services/scoutsuite.py`. The writer combines this filename with `scoutsuite-report` using `os.path.join` without sanitization or a resolved-path containment check. A traversal filename therefore writes the supplied JSON outside the intended report directory. ...

Versions of socfortress CoPilot the record lists as affected:

- < 0.1.77

What we do not know yet

- Whether anyone is exploiting this; the record is new and CISA does not list it.
- Whether a login is really needed: the description names admin and analyst users, the score says none.
- The release date and notes for 0.1.77; the sources do not give them.
- Whether a workaround exists short of updating.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 31 October 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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", "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-2026-61738: score 10, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H As the CVE record gives it.

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	None	No one has to do anything.
Scope	Changed	Damage reaches beyond 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
30 October 2026	CVE record published by GitHub.

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
CoPilot before 0.1.77 whose interface or API is reachable from the internet	Medium	This week; restrict access first
CoPilot before 0.1.77 reachable only from an internal network	Medium	This week or the next patch cycle
CoPilot before 0.1.77 where only a few trusted admins hold accounts	Medium	Next patch cycle
CoPilot at 0.1.77 or later	Low	Confirm the version in writing
You do not run CoPilot	None	None for this CVE

Appendix 4. Definition of done

- Every socfortress CoPilot you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-61738: <https://www.cve.org/CVERecord?id=CVE-2026-61738>
- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Advisory or release notes read: github.com/socfortress/CoPilot/security/advisories/GHSA-q3: <https://github.com/socfortress/CoPilot/security/advisories/GHSA-q3g8-3cf7-744f>
- Reference in the CVE record: [github.com](https://github.com/socfortress/CoPilot/pull/940): <https://github.com/socfortress/CoPilot/pull/940>
- Reference in the CVE record: [github.com](https://github.com/socfortress/CoPilot/pull/941): <https://github.com/socfortress/CoPilot/pull/941>
- Reference in the CVE record: [github.com](https://github.com/socfortress/CoPilot/commit/1881ef8d28bc7f45ffa88d7ba4fcca7302355508): <https://github.com/socfortress/CoPilot/commit/1881ef8d28bc7f45ffa88d7ba4fcca7302355508>