contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

ProFTPD exploited

CVE-2015-3306 · on CISA's exploited list since 8 October 2026

Analysis Report

If you run ProFTPD with the mod_copy module, treat this as overdue: CISA's date of 11 October 2026 has passed. First find out whether ProFTPD runs anywhere on your estate; if it does not, you can …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 10.0**	STATUS	On CISA's exploited list; due 11 October 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/proftpd-cve-2015-3306

The bottom line

> *If you run ProFTPD with the mod_copy module, treat this as overdue: CISA's date of 11 October 2026 has passed. First find out whether ProFTPD runs anywhere on your estate; if it does not, you can stop reading.*

At a glance

Fact	Detail
Product	ProFTPD (CVE-2015-3306)
Severity	Critical: 10 (CVSS 3.1)
CISA	On its exploited list since 8 October 2026. Deadline for US federal agencies: 11 October 2026.
Chance of exploitation (EPSS)	0.99, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Debian proftpd-dfsg 1.3.4a-5+deb7u3 (wheezy), 1.3.5-1.1+deb8u1 (jessie), 1.3.5-2 (stretch, sid), 19 May 2015. No upstream fixed version is named.
Who looks first	Anyone who runs a ProFTPD server, including one bundled in a Debian-based system. The record names version 1.3.5 and the mod_copy module. It lists no wider version range.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run ProFTPD on any server, appliance or hosting account?	Nothing to do for this CVE.	Check whether mod_copy is loaded (next question).
Is the mod_copy module loaded in your ProFTPD configuration?	The described flaw is not reachable through this module. Record the check and move on.	Check the version and package (next question).
Is your version 1.3.5, or a Debian package older than the fixed ones listed?	Ask your provider to confirm the fix in writing.	Update now, or switch mod_copy off until you can.

Can anyone untrusted, such as the internet, reach the FTP service?	Lower urgency, but still patch. Any internal user could use it.	Restrict access to known addresses today, then patch.

What it is

The record says a remote attacker can read and write arbitrary files using the site cpfr and site cpto commands of the mod_copy module. Debian's advisory says no login is needed and that running code is possible.

Why it matters

Our reading is that this flaw gives an attacker file access without a login, which makes it useful for stealing data, changing files or planting something on the server. The record scores it 10 on CVSS 3.1. The weakness is CWE-284 Improper Access Control. The advisory dates from 2015, so old, unmaintained FTP servers are the likely place for it to remain.

What the vendor's advisory says

We read one page on lists.debian.org. In short:

- Debian's advisory DSA-3263-1 of 19 May 2015 says mod_copy let unauthenticated users copy files around on the server, and possibly execute arbitrary code.
- The advisory names fixes for three Debian releases: 1.3.4a-5+deb7u3 for wheezy, 1.3.5-1.1+deb8u1 for jessie, and 1.3.5-2 for stretch and sid.
- The advisory recommends upgrading your proftpd-dfsg packages. It names no workaround.

Things people will get wrong

- "We only use FTP for harmless files." The record says an attacker can read and write arbitrary files, not only the FTP area. Debian says running code is possible.
- "It needs a valid account." Debian's advisory says unauthenticated users could use the copy commands.
- "A 2015 flaw must be patched already." CISA lists it as exploited. Old servers that are never updated stay exposed.

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 where ProFTPD runs

- List every server, appliance and hosting account that offers FTP. Ask your provider if unsure.
- Check the installed version and whether mod_copy is loaded.

```
proftpd -v
```

Step 2: Reduce exposure

- Limit access to the FTP service to known addresses until it is patched.
- Switch mod_copy off if you do not use it. The record's attack depends on this module.

Step 3: Patch

- Install the Debian package version listed for your release, or a newer one.
- If you use another distribution, ask its vendor for the fixed version. No source here names one.

Step 4: Check for signs of misuse

- Review FTP logs for site cpfr and site cpto commands you cannot explain.
- Check for files changed or added that nobody on your side made.

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 ProFTPD (CVE-2015-3306, the mod_copy flaw) and where. Please tell us each server that runs it, the exact version, and whether mod_copy is loaded. Debian's advisory lists fixes: 1.3.4a-5+deb7u3 (wheezy), 1.3.5-1.1+deb8u1 (jessie) and 1.3.5-2 (stretch, sid). CISA's date of 11 October 2026 has passed, so please treat this as urgent. Please confirm the version and the fix to us in writing by the end of this week.*

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:

- FTP log entries showing site cpfr or site cpto commands, especially from addresses you do not recognise.
- Files in unexpected places, or changed recently, that the FTP service account could write to.

The weakness behind it

CISA's entry classes this as CWE-284 (Improper Access Control).

The sources, in their words

CISA's catalogue entry:

> *ProFTPD contains an improper access control vulnerability that could allow remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.*

The CVE record, published by Mitre on 18 May 2015:

> *The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.*

The record gives no version ranges. Use the vendor's advisory for the affected versions.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which upstream ProFTPD release fixes this; the sources here name only Debian package versions.
- Whether versions other than 1.3.5 are affected; the record lists no version ranges.
- Which systems CISA saw attacked, or how.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 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", "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-2015-3306: 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. 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	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
18 May 2015	CVE record published by Mitre.
8 October 2026	CISA added it to its list of exploited vulnerabilities.
11 October 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
A ProFTPD server with mod_copy loaded, reachable from the internet	High	Now; CISA's window has already passed
A ProFTPD server with mod_copy, reachable only from your internal network	Medium	This week
ProFTPD installed but mod_copy not loaded	Low	Next patch cycle

An old Debian-based host running proftpd-dfsg that nobody maintains	High	Now; confirm the package version first
No ProFTPD anywhere on your estate	None	None for this CVE

Appendix 4. Definition of done

- Every ProFTPD 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.
- 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-2015-3306: https://www.cve.org/CVERecord?id=CVE-2015-3306
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: lists.debian.org/debian-security-announce/2015/msg00154.html: https://lists.debian.org/debian-security-announce/2015/msg00154.html
- Reference in the CVE record: www.exploit-db.com: https://www.exploit-db.com/exploits/36803/
- Reference in the CVE record: www.exploit-db.com: https://www.exploit-db.com/exploits/36742/