contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

ONLYOFFICE Docs exploited

CVE-2021-3199 · on CISA's exploited list since 8 October 2026

Analysis Report

If you run ONLYOFFICE Docs (Document Server) with JWT on, act now: CISA's date of 11 October 2026 has already passed. First find out whether it runs anywhere and which version; before 5.6.3 is …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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/onlyoffice-docs-cve-2021-3199

The bottom line

> *If you run ONLYOFFICE Docs (Document Server) with JWT on, act now: CISA's date of 11 October 2026 has already passed. First find out whether it runs anywhere and which version; before 5.6.3 is affected. If you do not run it, stop reading.*

At a glance

Fact	Detail
Product	ONLYOFFICE Docs (CVE-2021-3199)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 8 October 2026. Deadline for US federal agencies: 11 October 2026.
Chance of exploitation (EPSS)	0.30, 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	No source we read names a fixed version
Who looks first	Anyone running ONLYOFFICE Document Server, called ONLYOFFICE Docs by CISA, with JWT turned on. Check first any copy that people outside your firm can reach.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you or your IT provider run ONLYOFFICE Docs or Document Server anywhere?	Nothing to do for this CVE.	Find the version (next question).
Is the version before 5.6.3?	The record does not list it as affected; keep a note of the version.	Treat it as affected and go on.
Is JWT turned on for that server?	The record names JWT as a condition; confirm with your provider before you rely on that.	The stated condition is met; go on.
Can anyone outside your firm reach the server over the network?	Lower urgency, but still update it.	Restrict access now, then update.

What it is

The record says an attacker can send a crafted image upload request to the server's /upload path. A /.. sequence in a parameter lets it step outside the intended folder (CWE-22). The record says this can lead to remote code execution, meaning the attacker runs commands on the server.

Things people will get wrong

- "It is a 2021 flaw, so it is long dead." CISA lists it as exploited, and any copy still before 5.6.3 stays in range however old the record is.
- "JWT is on, so uploads are protected." The record names JWT use as the condition under which the flaw occurs, not as a protection.
- "We use it through another product, so it is not ours." The sources do not say how it is packaged. Ask your provider whether a copy runs on your behalf.

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 versions you run

- Ask your IT provider or supplier whether ONLYOFFICE Docs or Document Server runs anywhere on your estate.
- Record each version, as the record names versions before 5.6.3.

```
docker ps --format '{{.Names}} {{.Image}}' | grep -i onlyoffice
dpkg -l | grep -i onlyoffice
rpm -qa | grep -i onlyoffice
```

Step 2: Reduce exposure

- Take any affected copy off the internet, or limit access to the people who need it, until it is updated.
- Do this first for copies that people outside your firm can reach.

Step 3: Update

- Move to a current release from the vendor. The sources name no fixed version beyond the record's "before 5.6.3", so get the target from the vendor.
- Ask for the new version in writing.

Step 4: Check for signs of misuse

- Review web server and application logs for upload requests containing /.. sequences.
- If any are found, treat the server as possibly compromised and involve your provider.

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, CISA lists CVE-2021-3199, a path traversal flaw in ONLYOFFICE Docs (Document Server) that the record says can allow remote code execution when JWT is used. The record names versions before 5.6.3 as affected. Please tell us whether we run it anywhere, directly or through a supplier, and which version. If so, please update it and check its logs for unusual upload requests. Please confirm the version and the fix in writing by a date you suggest this week. Thank you.*

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:

- Upload requests in web or application logs whose paths contain /.. sequences.
- Files in the server's program folders that you did not put there or that changed unexpectedly.
- Unexpected outbound connections from the document server.

The weakness behind it

CISA's entry classes this as CWE-22 (Improper Limitation of a Pathname to a Restricted Directory).

The sources, in their words

CISA's catalogue entry:

> *ONLYOFFICE Docs contains a path traversal vulnerability that can occur when JWT is used, via a /.. sequence in an image upload parameter and could allow for remote code execution.*

The CVE record, published by Mitre on 22 January 2021:

> *Directory traversal with remote code execution can occur in /upload in ONLYOFFICE Document Server before 5.6.3, when JWT is used, via a /.. sequence in an image upload parameter.*

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

- The sources do not name a fixed version or what the fix changed.
- The sources do not say how attacks were carried out in practice or who was targeted.
- It is not stated whether a default or weak JWT secret is needed for an attack to work.
- 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", "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-2021-3199: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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	None	No one has to do anything.
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
22 January 2021	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
Server on a version before 5.6.3 with JWT on, reachable from the internet	High	Now; CISA's date has passed
Affected version with JWT on, reachable only from your internal network	Medium	This week
Version unknown, because a supplier or provider runs it for you	Medium	Ask this week

Version 5.6.3 or later	Low	Next patch cycle
You do not run ONLYOFFICE Docs	None	None for this CVE

Appendix 4. Definition of done

- Every ONLYOFFICE Docs 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-2021-3199: https://www.cve.org/CVERecord?id=CVE-2021-3199
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: github.com/moehw/poc_exploits/blob/master/CVE-2021-3199/po: https://github.com/moehw/poc_exploits/blob/master/CVE-2021-3199/poc_uploadImageFile.py
- Reference in the CVE record: github.com: https://github.com/ONLYOFFICE/DocumentServer/blob/903fe5ab7a275bd69c3c3346af2d21cf87ebeabf/CHANGELOG.md#563
- Reference in the CVE record: github.com: https://github.com/nola-milkin/poc_exploits/blob/master/CVE-2021-3199/poc_uploadImageFile.py
- Reference in the CVE record: github.com: https://github.com/moehw/poc_exploits/tree/master/CVE-2021-3199/poc_uploadImageFile.py