contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Fortinet FortiMail exploited

CVE-2026-104286 · on CISA's exploited list since 1 October 2026

Analysis Report

If you run FortiMail yourself (not FortiMail Cloud), act today: CISA's date of 4 October 2026 has passed. First turn off the IBE service or cut internet access to webmail, then upgrade. FortiMail ...

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 4 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/fortinet-fortimail-cve-2026-104286

The bottom line

> *If you run FortiMail yourself (not FortiMail Cloud), act today: CISA's date of 4 October 2026 has passed. First turn off the IBE service or cut internet access to webmail, then upgrade. FortiMail Cloud customers can stop reading.*

At a glance

Fact	Detail
Product	Fortinet FortiMail (CVE-2026-104286)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 1 October 2026. Deadline for US federal agencies: 4 October 2026.
Chance of exploitation (EPSS)	0.05, 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	FortiMail 8.0.2, 7.6.7 and 7.4.9 (or above). 7.2.10 is described as upcoming. 7.0 has no fixed release named: migrate. Vendor advisory, updated 7 October 2026.
Who looks first	Anyone running their own FortiMail appliance or virtual machine on 8.0, 7.6, 7.4, 7.2 or 7.0, especially if webmail or the IBE service can be reached from the internet.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run FortiMail yourself, as an appliance or virtual machine?	Nothing to do for this CVE.	Check whether it is FortiMail Cloud (next question).
Is your FortiMail the vendor-hosted FortiMail Cloud service?	Check the version (next question).	The vendor says it fixed Cloud on 5 October 2026. Nothing to do.
Is your version in a range listed as affected, with no fix applied yet?	You are on a fixed release. Confirm it in writing, then check the logs.	Reduce exposure now, then upgrade.

Is the IBE service on, or is webmail reachable from the internet?	The exposure is lower. Still upgrade, since the vendor's workarounds are not a fix.	Apply a workaround today, then upgrade.

What it is

An attacker with no login can send crafted HTTP or HTTPS requests to FortiMail and write arbitrary files on the underlying system. The vendor's advisory says this has been exploited in the wild and rates it Critical, CVSS 9.8.

Why it matters

The advisory says the flaw lets an unauthenticated attacker write files on the underlying system, and it lists the impact as executing unauthorised code or commands. Our reading is that a mail gateway is a useful foothold: it sits at the network edge and handles all inbound mail. The vendor's own indicators include a changed cron entry and a new archive account that sends data to a remote address. A low EPSS figure should not delay action when exploitation is already reported.

What the vendor's advisory says

We read one page on fortiguard.fortinet.com. In short:

- The vendor's advisory says fixes are in 8.0.2, 7.6.7 and 7.4.9 or above. 7.2.10 is described as upcoming.
- FortiMail 7.0, all versions, has no fixed release named. The advisory says to migrate to a fixed release.
- Workaround 1, from the advisory: switch the IBE service off in the GUI or with the CLI setting for IBE status.
- Workaround 2: block internet access to the webmail interface, or limit it to trusted private networks.
- Workaround 3: if a web application firewall sits in front, block POST requests to the IBE path that contain '../'.

Things people will get wrong

- "The score is 9.8 on paper, so it will not matter for us." The vendor's advisory says it is exploited in the wild and needs no login. The temporal score of 8.8 is still high.
- "We switched IBE off, so we are safe." That is a workaround, not a fix. The advisory also says to upgrade, and the flaw may already have been used before you switched it off.
- "Upgrading to 7.2.9 fixes it." 7.2.0 through 7.2.9 are listed as affected. The advisory names 7.2.10 as upcoming, not released.

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

- List every FortiMail you manage and note whether it is self-run or FortiMail Cloud.
- Compare each version with the affected ranges in the advisory.

```
get system status
show system encryption ibe
```

Step 2: Reduce exposure

- Turn the IBE service off, or limit webmail to trusted private networks, as the advisory says.
- If a web application firewall sits in front, block POST requests to the IBE path that contain '../'.

Step 3: Upgrade

- Move to 8.0.2, 7.6.7 or 7.4.9, or above, as the advisory says.
- On 7.2, wait for 7.2.10. On 7.0, migrate to a fixed release.

Step 4: Check for signs of use

- Look for the indicators in the vendor's advisory: cron entries, new archive accounts, IBE decryption errors.
- If you find any, treat the appliance as compromised and follow CISA's forensic guidance.

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 confirm our exposure to CVE-2026-104286, a path traversal flaw in Fortinet FortiMail that the vendor says is being exploited. Please tell us whether we run FortiMail ourselves or use FortiMail Cloud, and which version each system runs. The fixed releases are 8.0.2, 7.6.7 and 7.4.9 or above. Please disable the IBE service or restrict webmail access now, then upgrade. Please also check for the indicators in the vendor's advisory. We would like written confirmation of the versions and the fix 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:

- Cron entries in the system event log that run a script from an unfamiliar path.
- An archive account you did not create, sending files to a remote address.
- IBE errors about invalid Base64 encoding, or internal users failing to log in.

The weakness behind it

The record classes this as CWE-22 (Improper Limitation of a Pathname to a Restricted Directory).

The sources, in their words

CISA's catalogue entry:

> *Fortinet FortiMail contains a path traversal and an improper neutralization of NULL byte or NULL character vulnerability that may allow an unauthenticated attacker to write arbitrary files on the underlying system via crafted HTTP or HTTPS requests.*

The CVE record, published by Fortinet on 1 October 2026:

> *An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2.0 through 7.2.9, FortiMail 7.0 all versions may allow an unauthenticated attacker to write arbitrary files on the underlying system via crafted HTTP or HTTPS requests.*

Versions of Fortinet FortiMail the record lists as affected:

- 8.0.0 through 8.0.1

- 7.6.0 through 7.6.6
- 7.4.0 through 7.4.8
- 7.2.0 through 7.2.9
- 7.0.0 through 7.0.9

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 say how many systems have been compromised or how the attacks started.
- No release date is given for FortiMail 7.2.10.
- The record does not name a fixed 7.0 release, only that you should migrate.
- The sources do not say whether the IBE workaround removes all exposure.
- 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-2026-104286: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C` 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
1 October 2026	CVE record published by Fortinet.
1 October 2026	CISA added it to its list of exploited vulnerabilities.
4 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
Self-run FortiMail on an affected version, with IBE or webmail open to the internet	High	Today: workaround now, upgrade as soon as possible
Self-run FortiMail on an affected version, webmail limited to a trusted private network	Medium	This week, upgrade
FortiMail 7.0, any version, with no fixed release named	High	Plan the migration now; use the workarounds meanwhile

Self-run FortiMail already on 8.0.2, 7.6.7 or 7.4.9 or later	Low	Check the logs once, then no further action
FortiMail Cloud only	None	None for this CVE

Appendix 4. Definition of done

- Every Fortinet FortiMail 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-2026-104286: https://www.cve.org/CVERecord?id=CVE-2026-104286
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: fortiguard.fortinet.com/psirt/FG-IR-26-175: https://fortiguard.fortinet.com/psirt/FG-IR-26-175