

HiveForce Labs

# THREAT ADVISORY



## VULNERABILITY REPORT

### **Fortinet FortiMail Zero-Day Exploited to Write Arbitrary Files**

Date of Publication

October 6, 2026

Admiralty Code

A1

TA Number

TA2026291

# Summary

**First Seen:** October 1, 2026  
**Affected Products:** Fortinet FortiMail  
**Impact:** Fortinet FortiMail is affected by CVE-2026-104286, a critical path traversal flaw (CVSS 9.8) in its web interface. It lets unauthenticated attackers write arbitrary files on the underlying system through crafted HTTP or HTTPS requests. The flaw was exploited in the wild as a zero-day and enables root-level command execution and mail theft through rogue archive accounts. The flaw is now patched, and organizations should upgrade immediately or disable the IBE service until they can.

## CVE

| CVE             | NAME                                            | AFFECTED PRODUCT   | ZERO-DAY                                                                             | CISA KEV                                                                              | PATCH                                                                                 |
|-----------------|-------------------------------------------------|--------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| CVE-2026-104286 | Fortinet FortiMail Path Traversal Vulnerability | Fortinet FortiMail |  |  |  |

# Vulnerability Details

## #1

Fortinet FortiMail is a secure email gateway that filters inbound and outbound mail for spam, malware, and data loss, and it commonly sits at the network edge where its web interfaces face the internet. CVE-2026-104286 is a critical path traversal flaw (CWE-22) compounded by improper neutralization of NULL bytes (CWE-158) in the FortiMail web GUI, rated 9.8 on CVSS v3.1. The vendor confirms the flaw was exploited in the wild as a zero-day.

## #2

The flaw arises because the web interface does not properly constrain file paths or neutralize NULL characters supplied in HTTP or HTTPS requests, letting an unauthenticated remote attacker send crafted requests that write arbitrary files outside the intended directory on the underlying system. The vendor's workaround, which targets the Identity-Based Encryption (IBE) service and POST requests to the /ibe endpoint containing traversal sequences, identifies IBE as the exposed code path. FortiMail 8.0.0 through 8.0.1, 7.6.0 through 7.6.6, 7.4.0 through 7.4.8, and 7.2.0 through 7.2.9 are affected.

## #3

Indicators released by the vendor show root-level cron execution of shell commands referencing the /migadmin directory, administrator sessions logging out from a null interface, and a rogue archive account configured to ship rotated mail archives to an attacker-controlled server. Successful exploitation therefore allows execution of unauthorized code or commands, full control of the mail gateway, and silent theft of corporate email.

## #4

No threat actor attribution, victim count, or exploitation timeline has been made public. The flaw is now patched in 8.0.2, 7.6.7, and 7.4.9, while 7.2 deployments must migrate to a supported branch; until upgrades are complete, disabling IBE, restricting webmail exposure, and hunting for the published indicators remain essential.

# Vulnerability

| CVE ID          | AFFECTED PRODUCTS                                                                                                 | AFFECTED CPE                                | CWE ID          |
|-----------------|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-----------------|
| CVE-2026-104286 | Fortinet FortiMail<br>8.0.0 through 8.0.1,<br>7.6.0 through 7.6.6,<br>7.4.0 through 7.4.8,<br>7.2.0 through 7.2.9 | cpe:2.3:a:fortinet:fort<br>mail:*:*:*:*:*:* | CWE-22, CWE-158 |

## Recommendations

- 

**Upgrade FortiMail Without Delay:** Upgrade FortiMail 8.0 to 8.0.2 or above, 7.6 to 7.6.7 or above, and 7.4 to 7.4.9 or above. Appliances on the 7.2 branch have no fix within that branch and must be migrated to 7.4 or above. Confirm the running build on every appliance after the upgrade, including HA peers and virtual instances.
- 

**Disable the IBE Service Until Patched:** Where an upgrade cannot be applied immediately, turn off Identity-Based Encryption in the GUI under Encryption, IBE, by setting IBE Service to off, or from the CLI by running "config system encryption ibe", "set status disable", and "end". This closes the code path the vendor identifies as exploitable, so coordinate the change with mail operations because it may affect users who rely on IBE-encrypted mail.
- 

**Remove Internet Exposure of the Webmail Interface:** Disable access to the FortiMail webmail interface from the internet or limit it to trusted private networks only. Appliances whose web interfaces are reachable from the internet, particularly those with IBE enabled, should be remediated first.



**Block Traversal Attempts at the WAF:** If a web application firewall sits in front of FortiMail, block POST requests to /ibe that contain the ../ sequence and log every match as a potential exploitation attempt for follow-up investigation.



**Preserve Evidence Before Remediation:** Capture system event logs, encryption logs, configuration backups, and, where possible, forensic images of each appliance before upgrading or reconfiguring it, since remediation can overwrite the artifacts needed to establish whether and when a device was compromised.



**Hunt for Published Indicators:** Search FortiMail logs and network telemetry for connections to the IP addresses listed in the IoC section. Review system event logs for cron entries running /bin/sh as root with references to /migadmin, administrator logouts recorded from a null interface, and archive accounts such as archive234 configured with a remote destination, and review encryption logs for IBE decrypter BufferException errors reporting invalid Base64 encoding at position 0 alongside failed logins by wildcard internal users.



**Remove Rogue Configuration and Rotate Credentials:** Audit archive account settings and delete any account that sends archives to an unrecognized remote server, rotate administrator credentials, review all administrative accounts for unauthorized changes, and treat any mail archived to attacker infrastructure as exposed. Where compromise is confirmed, rebuild the appliance from a known-good image rather than relying on the upgrade alone.



**Continuously Monitor Edge Appliances:** Forward FortiMail system, administrative, and encryption logs to a central SIEM, and alert on changes to archiving configuration, scheduled tasks, and administrator sessions, as well as on outbound connections from the mail gateway to unfamiliar hosts.



# Potential MITRE ATT&CK TTPs

| Tactic         | Technique                                        | Sub-technique                               |
|----------------|--------------------------------------------------|---------------------------------------------|
| Initial Access | <u>T1190</u> : Exploit Public-Facing Application |                                             |
| Execution      | <u>T1053</u> : Scheduled Task/Job                | <u>T1053.003</u> : Cron                     |
|                | <u>T1059</u> : Command and Scripting Interpreter | <u>T1059.004</u> : Unix Shell               |
|                | <u>T1574</u> : Hijack Execution Flow             | <u>T1574.006</u> : Dynamic Linker Hijacking |
| Collection     | <u>T1114</u> : Email Collection                  | <u>T1114.003</u> : Email Forwarding Rule    |
| Exfiltration   | <u>T1029</u> : Scheduled Transfer                |                                             |



## Indicators of Compromise (IOCs)

| TYPE     | VALUE                                                                                                                                                                                                                                                          |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv4     | 79[.]141[.]169[.]187,<br>45[.]129[.]0[.]192                                                                                                                                                                                                                    |
| Username | archive234                                                                                                                                                                                                                                                     |
| MD5      | 64c90a00c7fda4d5c7973ed64c25783a,<br>5241738a3e9988404239e12243f6d35b,<br>ae0ea6502d3fa5f0664bceb73189eb54,<br>f90fa81a5f521d785f2b2f765e3ab897,<br>61af1c4bce1c2eebc8ff689ca5337791,<br>8eb64f25d2a8e18e05aae058629473cf,<br>49a7156a7d043cc8f9f680579db22f86 |



| TYPE      | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SHA256    | 8015f34dc84922b03688399d7f9fe7a00361789f7e420c7e2a2cdb23e75cef84,<br>77324ac428bde86d351fc5fc06f6d64a6bfe737dfb2743df1d4c5ac2418a5b6,<br>7a6cea9f5c9e2e9994d4e3c4da73f86cf5acd05ea5d312c066c9d1dafd69ee38,<br>4000276a150a165d3c2537d1e19fb393c4de8333076a16655e28059cae82157b,<br>703e97c64e61e41dc3aaba580d82bb2aa7b6a11b54ee6fb467ed5d5a3bffdef5,<br>8953ec7960b09f544a880b072ad4e6cfda7a8303f486251d3478dcfdfbac23b6,<br>d6fe51c22b91776f4c961ea58bcac5917f15d560a619d7ce726d3d51795609d3 |
| File Path | /data/lib/liblog.so,<br>/bin/smit,<br>/data/bin/webconsole,<br>/data/bin/mailexservice,<br>/data/etc/httpd.conf,<br>/data/etc/ld.so.preload,<br>/data/migadmin.tar.gz                                                                                                                                                                                                                                                                                                                         |

## Patch Link

<https://fortiguard.fortinet.com/psirt/FG-IR-26-175>

## References

<https://fortiguard.fortinet.com/psirt/FG-IR-26-175>

<https://watchtower.com/intelligence/fortinet-fortimail-cve-2026-104286-faq/>

<https://ccb.belgium.be/advisories/warning-actively-exploited-fortimail-vulnerability-patch-immediately>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

**October 06, 2026 • 11:15 PM**

© 2026 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)