

FortMail パス名を指定されたディレクトリ内に適切に制限できていない問題について

Fortinet 社の PSIRT(Product Security Incident Response Team)より Critical として、以下の情報が公開されましたので、以下の通りご報告させていただきます。

概要：

パストラバーサル（CWE-22）およびNULLバイト／NULL文字の処理不備（CWE-158）に関する脆弱性が存在します。この脆弱性を悪用すると、認証されていない攻撃者が、細工した HTTP/HTTPS リクエストを送信することで、対象システム上に任意のファイルを書き込める可能性があります。

また、本脆弱性は実際の攻撃で悪用されていることが報告されているため、対策バージョンへのアップグレード、または下記の回避策を速やかに適用することが推奨されています。

深刻度：

CVSS：9.8（致命的）

CVE ID：

CVE-2026-104286

影響：

不正なコードやコマンドを実行する

バージョン	影響のあるバージョン	対策バージョン
FortiMail 8.0	8.0.0 ～ 8.0.1	8.0.2以上へのアップグレードしてください
FortiMail 7.6	7.6.0 ～ 7.6.6	7.6.7以上へのアップグレードしてください
FortiMail 7.4	7.4.0 ～ 7.4.8	7.4.9以上へのアップグレードしてください
FortiMail 7.2	7.2.0 ～ 7.2.9	7.4、またはそれ以上へのアップグレードしてください

回避策：

以下のCLIコマンドを使用して、IBE機能を無効化します。

```
config system encryption ibe
set status disable
end
```

代替策：

FortiMailの管理インターフェースへのインターネットからのアクセスを無効化するか、信頼できるプライベートネットワークからのアクセスのみに制限します。

侵害の痕跡 (IoC):

ファイル:

```
* [ADDED]/data/lib/liblog.so MD5 - 64c90a00c7fda4d5c7973ed64c25783a SHA256 -
8015f34dc84922b03688399d7f9fe7a00361789f7e420c7e2a2cdb23e75cef84
* [MODIFIED]/bin/smit MD5 - 5241738a3e9988404239e12243f6d35b SHA256 -
77324ac428bde86d351fc5fc06f6d64a6bfe737dfb2743dfd4c5ac2418a5b6a
* [ADDED]/data/bin/webconsole MD5 - ae0ea6502d3fa5f0664bceb73189eb54 SHA256 -
7a6cea9f5c9e2e9994d4e3c4da73f86cf5acd05ea5d312c066c9d1dafd69ee38
* [ADDED]/data/bin/mailservice MD5 - f90fa81a5f521d785f2b2f765e3ab897 SHA256 -
4000276a150a165d3c2537d1e19fb393c4de8333076a16655e28059cae82157b
* [MODIFIED]/data/etc/httpd.conf MD5 - 61af1c4bce1c2eebc8ff689ca5337791 SHA256 -
703e97c64e61e41dc3aaba580d82bb2aa7b6a11b54ee6fb467ed5d5a3bfffdef5
* [ADDED]/data/etc/ld.so.preload MD5 - 8eb64f25d2a8e18e05aae058629473cf SHA256 -
8953ec7960b09f544a880b072ad4e6cfda7a8303f486251d3478dcfdcfbac23b6
* [MODIFIED] /data/migadmin.tar.gz MD5 - 49a7156a7d043cc8f9f680579db22f86 SHA256 -
d6fe51c22b91776f4c961ea58bcac5917f15d560a619d7ce726d3d51795609d3
```

IPアドレスについて:

79[.]141.169.187

45[.]129.0.192

Logs:

```
- type=event subtype=system pri=debug user=system ui=cron msg="(root) CMD (/bin/sh
-c '0=/migadmin ...
- type=kevent subtype=admin pri=information user=admin ui=(null) action=logout
status=success reason=unknown msg="User admin logged out from (null).
- type=kevent subtype=config pri=information user=admin ui=cli module=unknown
submodule=unknown msg="Added 'archive234' to 'archive account' :
rotation-size[50]rotation-time[1]
rotation-hour[14]destination[remote]remote-ip[79.141.169.187]remote-username[arch
ive234]remote-password[***]remote-directory[/uploads] (user: admin, from: cli)"
- FortiMail::IBE::DecrypterMediaIn::DecrypterMediaIn(FortiMail::MediaIn&, const
FortiMail::IBE::KeyFinder&, const FortiMail::EmailAddress&, const
FortiMail::Buffer&, FortiMail::IBE::DecrypterMediaIn::Version): Caught
BufferException(2), BufferImpl.cpp:973, 'Invalid Base64 Encoding at pos 0.
Character=0x2a'
- Internal user *@domain.tld<mailto:*@domain.tld> failed to log in.
```

詳細は以下メーカ情報をご確認ください。

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

以上