■CVE-2026-31431 に関する暫定対処につきまして

2026 年 4 月 29 日に公開された CVE-2026-31431 につきまして、
多数のお問い合わせをいただいております。

本脆弱性につきましては、algif_aead を無効化することで暫定的な回避が可能と判断しております。
なお、無効化の方法は OS や kernel の構成により異なる場合がございます。
以下に、一例として弊社で確認している手順をご案内いたします。

※注意事項
・本手順の実施可否につきましては、必ず施設内のセキュリティご担当者様へご確認のうえ、個別環境に適した手順をご採用ください。
・本手順の実施に伴い発生した、個別環境に依存するトラブルにつきましては、サポートいたしかねます。
・本手順は、下記情報サイトの内容を参考に、弊社にて確認した暫定的な影響軽減策の一例です。
・algif_aead の無効化により、すべての環境で本脆弱性の影響が解消されることを保証するものではございません。
・恒久的な対処としては、修正版 kernel または関連パッケージの適用が必要となる場合がございます。

https://www.ipa.go.jp/security/security-alert/2026/alert20260501.html
https://access.redhat.com/security/cve/cve-2026-31431
https://ubuntu.com/security/CVE-2026-31431

RealComputing,inc.　rc-support@realcomputing.jp

■Rocky Linux 環境

※root ユーザーで実施が必要です。
※OS 再起動が含まれます。

・コマンド.1 - grub に blacklist を登録
grubby --update-kernel=ALL --args="initcall_blacklist=algif_aead_init"

・コマンド.2 - 上記反映の為、OS 再起動の実施
reboot

・コマンド.3 - OS 再起動後、以下のコマンドで反映を確認
cat /proc/cmdline | grep -o 'initcall_blacklist=algif_aead_init'

実行結果として initcall_blacklist=algif_aead_init の表示を確認し、
本手順は完了です。

■Ubuntu LTS 22.04 / 24.04 環境

※sudo su - コマンドでスーパーユーザーへスイッチするか、sudo 権限で実施が必要です。
※OS 再起動が含まれます。

・コマンド.1 - algif_aead モジュールのロード抑止設定を作成

/etc/modprobe.d/ 配下に disable-algif-aead.conf を作成し、下記 2 行を記述します。

```
install algif_aead /bin/false
blacklist algif_aead
```

コマンド実行例：

```
cat <<'EOF' | sudo tee /etc/modprobe.d/disable-algif-aead.conf
# CVE-2026-31431 temporary mitigation
install algif_aead /bin/false
blacklist algif_aead
EOF
```

※vi コマンド等でファイルを作成し、上記内容を記述する形でも問題ございません。

・コマンド.2 - OS 再起動の実施

```
# reboot
```

RealComputing,inc. rc-support@realcomputing.jp

・コマンド.3 - OS 再起動後、以下のコマンドで反映を確認.1

```
# lsmod | grep '^algif_aead' || echo "algif_aead is not loaded"
```

実行結果として algif_aead is not loaded の表示を確認

・コマンド.4 - OS 再起動後、以下のコマンドで反映を確認.2

```
# modprobe -n -v algif_aead
```

実行結果として install /bin/false の表示を確認し、
本手順は完了です。