お客様各位

2025 年 2 月 20 日
パスロジ株式会社
PassLogic サポートグループ

RADIUS の Message-Authenticator 属性について

平素より「PassLogic エンタープライズ版」をご利用いただき、誠にありがとうございます。
ご利用中の SSL-VPN や UTM 等の機器のファームウェアアップデートを実施した後、PassLogic との RADIUS 認証連携が正常に動作しないというお問い合わせを複数いただいております。
以下に対処方法等の情報を記載いたしますので、ご確認ください。

■ 原因

CVE-2024-3596 で説明されている RADIUS の脆弱性から保護するための対策として、SSL-VPN や UTM の機器側のファームウェアアップデートにより、Message-Authenticator 属性の検証が必須となったためです。

■ 対処方法

1）Red Hat 社の修正済み FreeRADIUS を認証サーバに適用

CVE-2024-3596 に対応した Red Hat 社の修正済み FreeRADIUS を PassLogic 認証サーバに適用してください。修正済み FreeRADIUS の入手方法など、詳細は Red Hat 社にご確認ください。
参考：https://access.redhat.com/security/cve/cve-2024-3596

2）/etc/raddb/radiusd.conf の security セクションに設定を追加

1）の修正済み FreeRADIUS を適用後、/etc/raddb/radiusd.conf の security セクションに以下の設定を追加してください。

設定例：

```
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
security {
...
require_message_authenticator = yes
limit_proxy_state = yes

}
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
```

■ 設定の補足説明

「require_message_authenticator」および「limit_proxy_state」両項目は、「auto」に設定することも可能です。しかし「auto」に設定した場合、最初のクライアントからのリクエストに基づい

て動的に yes/no の判定が行われるため、クライアント側からのリクエストの属性状況を把握できていない場合、予期せぬ RADIUS 認証リクエストの破棄が発生する可能性があります。
そのため、明示的に「yes」を設定することを推奨いたします。
なお、/etc/raddb/radiusd.conf の security セクションに上記の設定を記述しない場合、両項目はデフォルトで「auto」となります。
詳細は以下の URL をご確認ください。
https://www.freeradius.org/security/

弊社ではお客様の環境ごとに動作確認を行うことができませんので、上記の内容を参考に、貴社環境に合わせた事前検証を実施していただくよう、お願いいたします。

■ 設定反映方法

/etc/raddb/radiusd.conf を修正後、以下のコマンドを実行して radiusd を再起動し、設定を反映してください。

```
systemctl restart radiusd
```

以上、よろしくお願いいたします。