

お客様各位

株式会社日立ソリューションズ

Fortinet 製品ユーザサポート

FortiGate における RADIUS 認証が失敗する事象について(CSB-241001-1)

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

この度 Fortinet 社より、FortiOS のアップグレード後に、FortiGate における RADIUS 認証が失敗する事象がアナウンスされています。本件に該当する環境でご利用のお客様におかれましては、「3.対応策」をご確認いただき、ご対応くださいますようお願いいたします。

敬具

記

1. 事象と背景

RADIUS プロトコルの脆弱性(CVE-2024-3596)への FortiOS の対応(※)に伴い、FortiOS を「2.対象 OS とバージョン」に示したバージョンにアップグレードした際に、RADIUS サーバ側での RFC 3579(RADIUS 属性の message-authenticator)への対応状況に依存して、FortiGate における RADIUS 認証が失敗することがあります。

※ message-authenticator の検証の強制と、認識されていない proxy-state 属性を持つ RADIUS 応答の拒否を実施する変更が行われました。

2. 対象 OS とバージョン

以下にアップグレードした際に発生することがあります。

項	対象 OS (メジャーバージョン)	対象バージョン	備考
1	FortiOS 7.6 系	7.6.1 以降(予定)	7.6 系は弊社未リリースです。
2	FortiOS 7.4 系	7.4.5 以降	
3	FortiOS 7.2 系	7.2.10 以降	

3. 対応策

ご利用の環境に応じて、以下のいずれかで対応してください。

(1) RADIUS over TLS(RADSEC)を利用

RADIUS 認証において TLS を利用する場合、message-authenticator の検証は必須ではありません。このため、RADIUS 認証において TLS を利用可能な場合は、RADSEC を利用して対応してください。なお、FortiOS では 7.4 系から RADSEC に対応しています。

(2) message-authenticator に対応しているバージョンの RADIUS サーバを利用

RADIUS 認証において UDP または TCP のみが利用可能な(TLS が利用できない)場合は、message-authenticator の検証が必須となるため、RADIUS サーバ側で message-authenticator に対応しているバージョン(パッチ)を利用することで対応してください。

詳細、最新の情報については 以下の Fortinet 社のドキュメントをご参照ください。

Troubleshooting Tip: RADIUS authentication failure after the firmware upgrade to v7.2.10/v7.4.5

<<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-RADIUS-authentication-failure-after-the/ta-p/343112>>

以上