

# 【Accopsニュースレター】2026.9.24 【製品脆弱性情報】Accops HySecureの脆弱性について

2026/10/25 16:22:39

記事印刷

|        |                      |              |                       |
|--------|----------------------|--------------|-----------------------|
| 区分:    | ACCOPS FAQ::01. お知らせ | 投票:          | 0                     |
| ステータス: | 公開 (全員)              | 結果:          | 0.00 %                |
| 言語:    | ja                   | Last update: | 2026/09/25 - 11:22:27 |

キーワード

HySecure,脆弱性

症状 (公開)

問題 (公開)

解決 (公開)

Accops ニュースレター - 2026.9.24 -  
本日はAccops製品のニュースレターとして、Accops HySecureの脆弱性情報をご提供させていただきます。  
【 Accops HySecure Gateway のリモートコード実行の脆弱性 】  
■概要  
HySecure Gatewayのすべてのバージョンにおいて、深刻度「Critical（緊急）」の脆弱性が発見されました。  
脆弱性の詳細および解決策についてご案内いたします。  
■アドバイザリ詳細  
アドバイザリID : ASA-2026-0901  
発行日 : 2026-09-24  
深刻度 : Critical（緊急）  
■対象製品  
HySecure Gateway : 全てのバージョン  
■脆弱性の詳細  
Gatewayで使用する内部エージェントサービスに、認証を必要としないファイル書き込みの脆弱性が存在します。  
宛先パスおよびファイルタイプの検証が不十分であるため、リモートの未認証ユーザーがGateway上に任意のファイルを配置し、Accops Webサーバーの制限付きユーザー権限でそのファイルを実行することが可能になります。  
悪用（エクスプロイト）の試行時にアクセスされるパスには、以下のURIが含まれます  
/home/fes-bin/public  
■悪用の検知  
提供されるホットフィックスには、本脆弱性が悪用された形跡があるかどうかを確認する機能が含まれています。  
セキュリティ修正を適用した後、アップグレードログファイルを確認してください。  
脆弱性が悪用されていた場合、アップグレードログにその旨が記録されます。  
■影響を受ける製品  
HySecure Gatewayのすべてのバージョン  
■解決策  
上記のセキュリティ脆弱性を修正するためのホットフィックスが間もなくリリースされます。  
ホットフィックスは、HySecure Gatewayバージョン5.4および7.xで利用可能です。  
該当するホットフィックスを可能な限り早期に適用することを強く推奨いたします。  
詳細については製品サポートまでお問合せください。

Related Product, Service (公開)