【Accopsニュースレター】2026.5.3
セキュリティアドバイザリー(CVE-2026-31431:Copy Fail)について

2026/09/17 20:31:33

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:	2026/05/07 - 09:31:13

症状 (公開)

問題 (公開)

解決 (公開)

CVE-2026-31431：Linuxカーネルの脆弱性 – ローカル権限昇格のAccops製品への影響につきまして

2026年4月29日、Linuxカーネルのalgif_aeadユーザー空間暗号インターフェースに、CVE-2026-31431 (CVSS 7.8 HIGH)、別名「Copy Fail」の脆弱性が発見されました。

CVE：CVE-2026-31431
深刻度：7.8 (高)

■脆弱性の詳細：
Linuxカーネルの暗号化ユーザー空間API（AF_ALG）、特にAEAD暗号（algif_aead）には、splice()システムコールの不適切な処理に起因する脆弱性が存在します。
これにより、内部AEADリクエストオブジェクトが解放後、使用（use-after-free）状態になる可能性があります。
これにより、ローカルの非特権ユーザーが影響を受けるシステム上で権限を昇格できる可能性があります。

ローカルの非特権ユーザー（コンテナ内を含む）は、以下の手順でこの脆弱性を悪用できます。
• AF_ALGソケット（SOCK_SEQPACKET）を開く。
• AEAD暗号（例：authenc(hmac(sha256),cbc(aes))）にバインドする。
• 細工されたsendmsg()呼び出しを使用して悪意のあるリクエストを初期化する。
• splice()システムコールを使用して脆弱性をトリガーする。

■悪用成功の条件：
• CONFIG_CRYPTO_USER_API_AEADが有効になっているLinuxカーネルがコンパイルされている。
• 攻撃者がシステムへのローカルユーザーアクセス権（コンテナへのアクセス権を含む）を持っている。
• algif_aeadモジュールがロードされている、または自動ロード可能である。

Accops HySecureおよびAccops Reporting Server（ARS）はOracle
Linuxディストリビューションをベースとしており、
影響を受けるLinuxカーネルコンポーネントが含まれています。
この機能はアプリケーションでは使用されていませんが、脆弱なコンポーネントは基盤となるOSに存在します。

■影響を受ける製品
Accops HySecure Gateway：全バージョン
Accops Reporting Server (ARS)：全バージョン
Linux Shared Hosted Desktop (Ubuntu / CentOS / RHEL ベース)：全バージョン
Accops VDI (Linux ネイティブ)：全バージョン
Accops HyDesk デバイス (Ubuntu ベース OS)：全バージョン

■影響を受けない製品
Accops Workspace Client for Windows：Windows OS は影響を受けません
Accops Workspace Client for Mac：macOS は影響を受けません
Accops Workspace Client (全プラットフォーム)：クライアント側アプリケーション、カーネルに依存しません
Accops HyID Client (全プラットフォーム)：クライアント側アプリケーション、カーネルに依存しません
Accops HyWorks および HyLabs：Windows 上のクライアント側アプリケーション、カーネルに依存しません
Accops BioAuth：Windows 上のクライアント側アプリケーション、カーネルに依存しません

■現状での対応について
HySecure Gateway
数日中にリリースされる、セキュリティホットフィックスを適用してください。その他の影響を受けるシステム
緩和スクリプトを実行してください。
その後、システムを再起動してください。

■今後の解決策について
CVE-2026-31431の公開を受け、Accopsセキュリティチームは全製品ラインにおける影響を評価しました。
HySecure Gatewayについては、専用のセキュリティホットフィックスがリリースされますのでホットフィックスを適用してください。
その他の影響を受ける製品については、アップストリームベンダーから公式カーネルパッチがリリースされるまでの間、脆弱性を軽減するための緩和スクリプトを提供します。

この回避策は、カーネルの完全なアップグレードを必要とせずに、脆弱性の悪用を阻止します。
ディストリビューションベンダーが公式のカーネルパッチをリリース次第、更新されたガイダンスを提供いたします。

Related Product, Service (公開)