【Accopsニュースレター】2026.5.21
セキュリティアドバイザリー(Linux脆弱性対応)について

2026/09/17 20:28:32

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:	2026/05/21 - 13:21:15

症状 (公開)

問題 (公開)

解決 (公開)

本日はAccops製品のニュースレターとして、以前（2026.5.3/2026.5.8）に配信済みのセキュリティアドバイザリーについて、追加の情報をお届けいたします。
下記内容についてはすでに案内済みの内容も含まれております。
Linuxカーネルの脆弱性 - ローカル権限昇格（Copy Fail：CVE-2026-31431）と
（Dirty Frag：CVE-2026-43284 & CVE-2026-43500）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、脆弱性「Copy Fail」が発見されました。
CVE：CVE-2026-31431深刻度：7.8 (高)

また、2026年5月8日、Linuxカーネルに、SSHアクセス権限を持つローカルユーザーが不正にroot権限を取得できるゼロデイ脆弱性「Dirty Frag」が発見されました。
CVE：CVE-2026-43284 & CVE-2026-43500深刻度：7.1 (高)

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

■対応方法
HySecure Gateway
リリース済みのセキュリティホットフィックスを適用ください。
下記セキュリティホットフィックスについては非累積のホットフィックスとなりますので、
SH14のセキュリティホットフィックスが適用されている環境に、
下記のセキュリティホットフィックスを順番に適用頂きますようお願いいたします。
OS15：OSレベルのパッケージ更新およびCVE修正（OS16・OS17以外）
OS16：CVE-2026-31431：Copy Fail対応
OS17：CVE-2026-43284 & CVE-2026-43500：Dirty Frag対応

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。

■その他
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ています。
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)