テクノロジー ファイル処理任意 の コード実行 脆弱性の Oracle 外部で

Medium	**アドバイザリーID :** Cisco-SA-20110420-CVE-2011-0808 **初公開日 :** 2011-04-20 21:20 **最終更新日 :** 2012-07-14 13:02 **バージョン 3.0 :** Final **CVSSスコア :** 10.0 **回避策 :** Yes **Cisco バグ ID :** CSCtq29413	CVE-2011-0794 CVE-2011-0808

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Oracle フュージョン ミドルウェア アプリケーションによって使用する技術コンポーネントの Oracle は外部で非認証を可能にする可能性があるターゲットのシステムの任意 の コードを実行するために脆弱性がリモート攻撃者含まれています。

影響を受けたソフトウェアによって Lotus 1-2-3 スプレッドシート ファイル（WKS）および Microsoft キャビネット（CAB）ファイルの不正確な処理による脆弱性存在。 非認証はテクノロジー ライブラリの外部に頼るターゲットとされたユーザのアプリケーションを使用して悪意のあるファイルを表示するように確信によって、リモート攻撃者この脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者がユーザの特権の任意 の コードを実行することを可能にする可能性があります。

Oracle は脆弱性を確認し、更新済ソフトウェアをリリースしました。

この脆弱性を不正利用するために、攻撃者はターゲットとされたユーザを影響を受けたソフトウェアの悪意のあるファイルを開くように確信させる必要があります。 この目標を達成するために、攻撃者は社会工学手法を使用し、メールの添付データとして通信のインスタント メッセージか他のフォームによって悪意のあるファイルを、送信 するかもしれません。

ベンダーから記録する CVSS は ローカル攻撃者によって開発可能な部分的なアベイラビリティ インパクトを示します。 記録するこれは影響を受けたライブラリを使用してシステムに開発の間にエラーのアプリケーションか可能性のある 概要を開発するために影響を反映するかもしれません

。 ただし、このアラートに記述されているように、他のレポートはユーザの特権のシステムの任意 の コードを実行するのに非認証が、リモート攻撃者脆弱性を活用 する可能性があることを示します。 脆弱 なライブラリを使用するユーザのシステムの悪意のあるファイルを表示するように確信によって、攻撃者はターゲットとされたユーザの特権の影響を受けたシステムの任意 の コードを実行する可能性があります。

Cisco は CVSS スコアを通してその機能エクスプロイト コード存在を示します; ただし、コードは共用利用可能であると知られていません。

該当製品

修正済みソフトウェア

テクノロジー バージョン 8.3.2 および 8.3.5 の Oracle によって外部で提供されるライブラリに頼るアプリケーションは影響を受けています。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2011-Apr-20

利用規約