Sudo sudoedit ローカルコマンド特権拡大脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20100419-CVE-2010-1163 **初公開日 :** 2010-04-19 20:43 **最終更新日 :** 2015-01-31 05:30 **バージョン 5.0 :** Final **CVSSスコア :** 6.0 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2010-1163

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

Sudo は認証された可能性がある高度な特権の任意のコマンドを実行するために脆弱性が、ローカル攻撃者を可能にする含まれています。

不正確なパス解決によるコマンドと一致している間影響を受けたソフトウェアのエラーによるこの脆弱性存在。 **sudoedit** コマンドを実行する特権のローカル攻撃者は*ルート 特権*の任意のコマンドを実行するのにこの脆弱性を不正利用する可能性があります。 エクスプロイトは完全なシステム妥協という結果に終る可能性があります。

この脆弱性を不正利用する Proof-of-concept コードは共用利用可能です。

ベンダーはこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

脆弱性を不正利用するために、攻撃者はシステムにローカルアクセスをアクセスできるおよび **sudoedit** コマンドを実行する特別なアクセス許可を与える必要があります。 これらの必要条件の結果として、エクスプロイトのソースは影響を受けたシステムの現在のユーザに多分制限されます。 不正利用の成功はローカル攻撃者が全システム妥協の原因となる*ルート*として任意 shell コマンドを実行することを可能にする可能性があります。

正常であるこの脆弱性に関しては攻撃者はを含む PATH 環境変数が「」。あるコマンドを渡します そして **sudoedit** コマンドが含まれている他のディレクトリが含まれないため。 また、正常なエクスプロイトはディセーブルにされるべき *ignore_dot* または *secure_path sudoers* オプションを必要とします。

該当製品

Sudo は次のリンクで Security Advisory のこの脆弱性を確認しました: CVE-2010-1163

Cisco は次のリンクでバグID をリリースしました: CSCtg35974、CSCth37846、CSCtf18342 および CSCth87771

Red Hat は次のリンクで Security Advisory をリリースしました: RHSA-2010:0361

脆弱性のある製品

1.7.2p5 による Sudo バージョン 1.6.8 は脆弱です。

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。

回避策

管理者は適切な更新を加えるように助言されます。

管理者は信頼されたユーザにローカルアクセスを制限するように助言されます。

管理者は信頼できない ユーザに *sudo* 特権を許可しないように助言されます。

修正済みソフトウェア

Sudo は次のリンクで更新バージョンをリリースしました: sudo 1.6.9p22、1.7.2p6 またはそれ以降

CentOS パッケージはまたは **yum** コマンド **up2date** を使用して更新済である場合もあります。

Red Hat パッケージはまたは **yum** コマンド **up2date** を使用して更新済である場合もあります。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20100419-CVE-

2010-1163

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2010-Apr-19

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。