CiscoWorks Common Services 任意のコマンド実行脆弱性

Critical

アドバイザリーID : cisco-sa-20111019-cs

初公開日 : 2011-10-19 16:00

バージョン 1.0 : Final

CVSSスコア : 9.0

回避策 : Yes

Cisco バグ ID : CSCtt25535 , CSCtq64019 , CSCtq48990 , CSCtq63992 , CSCtq64011 , CSCtr23090

CVE-2011-3310

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

Microsoft ウィンドウのための CiscoWorks Common Services は認証される可能にする可能性があるシステム アドミニストレータの特権の影響を受けたシステムの任意のコマン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。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。

この脆弱性を軽減する回避策がありません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111019-cs で掲示されます。

注: 有効な Â は 2011 年 10月 18 日、Cisco Cisco PSIRT によって送達された Cisco Security Advisory および応答の現在の一覧を移動しました。 新しい場所は http://tools.cisco.com/security/center/publicationListing です。 また Ciscoセキュリティ（SIO）ポータルのシスコ製品および Services メニューからのこのページにナビゲートできます。 この遷移の後で、新しい Cisco Security Advisory および応答は新しい場所に送達されます。 URL が変更したが、セキュリティ 文書のコンテンツおよび脆弱性ポリシーは影響を与えられません。 Cisco は送達された セキュリティ脆弱性ポリシーに従ってセキュリティー の 脆弱性を表わし続けます。

該当製品

修正済みソフトウェア

この脆弱性は Microsoft ウィンドウで動作する CiscoWorks よくあるサービス ベース 製品のすべてのバージョンに影響を与えます

Common Services バージョン 4.1 および それ 以降はこの脆弱性から影響を受けません。

インストールされる根本的な Common Services バージョンによるこの脆弱性からデフォルト Common Services を用いる以下の CiscoWorksプロダクトは影響を受けます:

- **CiscoWorks LAN Management Solution**

  注: 3.2 以前の CiscoWorks LAN Management Solution バージョンはソフトウェアメンテナンスの終わりに達しました。 顧客は CiscoWorks LAN Management Solution のサポート対象バージョンへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。
- **Cisco Security Manager**

  注: 3.2 以前の Cisco Security Manager バージョンはソフトウェアメンテナンスの終わりに達しました。 顧客は Cisco Security Manager のサポート対象バージョンへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。
- **Cisco Unified Operations Manager**

  注: 2.3 以前の Cisco Unified オペレーション マネージャバージョンはソフトウェアメンテナンスの終わりに達しました。 顧客は Cisco Unified オペレーション担当マネージャーのサポート対象バージョンへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。
- **Cisco Unified Service Monitor**

  注: 2.2 以前の Cisco Unified サービス モニタバージョンはソフトウェアメンテナンスの終わりに達しました。 顧客は Cisco Unified サービス モニタのサポート対象バージョンへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。
- **CiscoWorks Quality of Service ポリシー マネージャ**

  注: 4.1 以前の CiscoWorks サービス品質（ QoS ） Policy Manager バージョンはソフトウェアメンテナンスの終わりに達しました。 顧客は CiscoWorks QoS Policy Manager のサポート対象バージョンへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。
- **CiscoWorks Voice Manager**

  注: 3.0 以前の CiscoWorks Voice Manager バージョンはソフトウェアメンテナンスの終わりに達しました。 顧客は CiscoWorks Voice Manager のサポート対象バージョンへのアッ

プグレードの支援に関しては Cisco サポート チームに連絡する必要があります。

脆弱性を含んでいないことが確認された製品

Solaris で動作するこの脆弱性から CiscoWorks よくあるサービス ベース 製品のすべてのバージョンは影響を受けません。

CiscoWorks Common Services バージョン 4.1 および それ 以降はこの脆弱性から影響を受けません。

以下の製品はまた確認された脆弱です:

- Cisco Prime LAN Management Solution バージョン 4.1 および それ 以降
- Cisco Security Manager バージョン 4.2 および それ 以降
- Cisco Unified Operations Manager 8.6 およびそれ以降
- Cisco Unified Service Monitor 8.6 およびそれ以降
- Solaris で動作する CiscoWorks LAN Management Solution のバージョン
- Solaris で動作する CiscoWorks QoS Policy Manager のバージョン
- Solaris で動作する CiscoWorks Voice Manager のバージョン

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

リビジョン 1.0	2011-October-19	初版リリース

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。