

CiscoWorks Internetwork Performance Monitorのリモートコマンド実行の脆弱性

severity アドバイザリーID : cisco-sa-20080313-ipm
初公開日 : 2008-03-13 18:00
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

Sun SolarisおよびMicrosoft Windowsオペレーティングシステム用のCiscoWorks Internetwork Performance Monitor(IPM)バージョン2.6には、認証されていないリモートユーザが任意のコマンドを実行できる脆弱性が存在します。この脆弱性に対する回避策はありません。Cisco では、該当するお客様用に、この問題に対応するソフトウェアを無償で提供しております。

このアドバイザリーは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080313-ipm> で公開されています。

該当製品

脆弱性のある製品

SolarisおよびWindowsオペレーティングシステム用のIPMバージョン2.6には脆弱性が存在します。

脆弱性を含んでいないことが確認された製品

IPMバージョン2.5以前およびIPMバージョン4.0には脆弱性はありません。これらの脆弱性を含むその他の Cisco 製品は現在のところ報告されていません。

詳細

CiscoWorks IPMは、ネットワークの応答時間と可用性を測定するトラブルシューティングアプリケーションです。CiscoWorks LAN Management Solution(LMS)バンドル内のコンポーネントとして使用できます。SolarisおよびWindows用のIPMバージョン2.6には、コマンドシェルをランダムに選択されたTCPポートに自動的にバインドするプロセスが含まれています。リモートの未認証ユーザは、Solarisシステムでは`casuser`権限を使用し、Windowsシステムでは`SYSTEM`権限を使用して、オープンポートに接続し、任意のコマンドを実行できます。この脆弱性は、[CVE-2008-1157](#)およびCisco Bug ID [CSCsj06260](#)([登録](#)ユーザ専用)に記載されています。

回避策

この脆弱性に対する回避策はありません。IPMバージョン2.6を実行しているシステム上のTCPポートへのネットワークアクセスを信頼できるシステムに制限することで、この脆弱性を軽減できます。管理者は、IPMの修正済みバージョンにアップグレードすることを強く推奨します。

ネットワーク内のCiscoデバイスに導入できる追加の緩和テクニックについては、このアドバイザリに関連するCisco適用対応策速報を参照してください。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080313-ipm>

修正済みソフトウェア

アップグレードを検討する場合は、<http://www.cisco.com/go/psirt> と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレードソリューションを確認してください。

この脆弱性は、SolarisおよびWindowsオペレーティングシステム用のIPMバージョン2.6 CSCsj06260パッチで修正されています。修正済みソフトウェアは次のサイトで入手できます。

<http://www.cisco.com/cgi-bin/tablebuild.pl/ipm-sol?psrtdcat20e2>

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center (TAC) または契約を結んでいるメンテナンス プロバイダーにお問い合わせください。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。この脆弱性は、お客様からシスコに報告されたものです。

URL

改訂履歴

リビジョン 1.0	2008年3月13日	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、単独の転載や意識を施した場合、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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。