VCO/4Kのリモートパスワード開示

severity

アドバイザリーID : cisco-sa-20001026-vco4k-password

初公開日 : 2000-10-26 22:00

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

Cisco VCO/4Kの脆弱性は、許可されたユーザのパスワードを、読み取り専用のSNMPクエリーに応答して簡単に復号化できる形式で公開します。

VCO/4Kソフトウェアバージョン5.1.4より前の現在サポートされているすべてのリリースには、この不具合があります。現在利用可能なバージョン5.1.4には、脆弱に暗号化されたパスワードの表示を防止する修正が含まれています。2000年12月初旬にリリース予定のバージョン5.2には、この修正に加え、パスワードの暗号化と処理に関する複数の改善が含まれています。

該当するVCO/4000のお客様には、無償のソフトウェアアップグレードが提供されます。この不具合は、VCO/4KのSNMPサービスへのアクセスを制限することで回避できます。

この脆弱性は、Cisco Bug ID **CSCds55790**で文書化されています。

他のシスコ製品はこの脆弱性の影響を受けません。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001026-vco4k-passwordから入手できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

Cisco VCO/4Kのソフトウェアバージョン5.1.4より前の現在サポートされているすべてのリリ

ースには、この不具合が原因で脆弱性が存在します。バージョン5.1.4は、2000年8月中旬にリリースされました。

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。

詳細

Cisco VCO/4K(Virtual Central Office 4000)は、統合メッセージングなどの音声サービスを提供するプログラム可能なスイッチで、有線または無線ネットワークのコアインフラストラクチャスイッチとして動作するか、または回線とパケットが混在するネットワークのゲートウェイとして動作します。VCO/4Kは、1998年11月にシスコが買収したSumma Fourによって開発されました。

VCO/4Kのユーザ名と暗号化されたパスワードは、ネットワーク上のSNMP(Simple Network Management Protocol)クエリーに応答してリモートで表示できます。ただし、パスワードは、簡単に復号化できる代替暗号を使用して暗号化されます。この不具合は、Cisco Bug ID **CSCds55790**で文書化されています。

VCO/4Kソフトウェアには、SNMPクエリーによるユーザ名と暗号化されたパスワードの取得を防止するためのパッチが適用されており、パスワードの暗号化は、Cisco IOSソフトウェアで使用可能な「Type 5」パスワードの暗号化に置き換えられています。タイプ5のパスワードは、安全な一方向ハッシュであるMD5に基づいており、代替暗号よりも不正開示に対する復元力が大幅に高くなっています。さらに、VCO/4Kへのアクセスの複数の形式に新しいパスワード暗号化が適用され、システムへのアクセス制御が全般的に改善されました。

回避策

SNMPクエリをVCO/4Kに制限することで脅威を減らすことができますが、修正済みソフトウェアの方がはるかに強力な保護を提供します。できるだけ早くVCO/4Kソフトウェアバージョン5.1.4にアップグレードし、利用可能になり次第バージョン5.2にアップグレードすることを強くお勧めします。

修正済みソフトウェア

Cisco VCO/4Kソフトウェアバージョン5.1.4には、SNMPクエリに対する応答で暗号化されたパスワードが返されなくなる部分修正が含まれています。このバージョンは2000年8月中旬に利用可能になりました。

2000-12-04リリースを予定しているバージョン5.2では、SNMPによるパスワードの不正開示が引き続き防止されており、Cisco IOSソフトウェアのType 5パスワード暗号化と同等のVCO/4Kパスワード暗号化処理の改善が含まれています。

不正利用事例と公式発表

この脆弱性は、@Stake, Inc.によってCisco PSIRTに報告され、お客様のネットワークの監査中に発見されました。

Cisco PSIRTでは、この脆弱性の悪用に関する情報は得られていません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001026-vco4k-password

改訂履歴

リビジョン 1.0	2000年10月26日	初回公開リリース

利用規約

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。