Cisco PIXの複数の脆弱性

アドバイザリーID : cisco-sa-20021120-pix-vulnerability
初公開日 : 2002-11-20 16:00
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 PIX Firewallは、ステートフルインスペクションファイアウォール、標準ベースのIP Security(IPsec)Virtual Private Networking(VPN)、侵入防御など、堅牢なエンタープライズクラスのセキュリティサービスを、コスト効率が高く導入が容易なソリューションで提供します。

修正が提供されているPIXファイアウォールについては、2つの脆弱性が解決されています。これらの脆弱性は、Cisco Bug ID CSCdv83490およびCSCdx35823に記載されています。

これらの脆弱性の影響を軽減するための回避策はありません。

シスコはこれら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ています。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20021120-pix-vulnerability で公開されています。

該当製品

脆弱性のある製品

脆弱性のあるリリースを実行し、特定の機能を使用しているすべてのPIXファイアウォールユニットが、これらの脆弱性の影響を受けます。

DDT：説明	影響を受けるリリ

	ース
CSCdv83490:Initial Contact Notify(INITIAL CONTACT NOTIFY)メッセージの処理中に、PIXでは、ピアとの重複するInternet Security Authentication Key Management Protocol(ISAKMP)Security Associations(ISAKMP SA)は削除されません。	6.0.3以前 6.1.3以前
CSCdx35823:Terminal Access Controller Access Control System Plus(TACACS+)またはRemote Authentication Dial-In User Service(RADIUS)を使用してHTTPトラフィック認証を行っている間にバッファオーバーフローが発生します。	5.2.8以前 6.0.3以前 6.1.3以前 6.2.1以前

使用しているソフトウェアリビジョンを確認するには、コマンドラインプロンプトでshow versionと入力します。

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。

詳細

0.CSCdv83490

ピアとユーザの認証に成功した時点でユーザがVPNセッションを確立すると、PIXはユーザとそのIPアドレスを関連付けるISAKMP SAを作成します。

攻撃者がログインしたユーザの接続をブロックし、ユーザと同じIPアドレスを使用してPIXへの接続を確立できるようになった場合、グループ事前共有キー(PSK)またはグループパスワードキーとも呼ばれるピア認証キーへのアクセス権をすでに持っていれば、ピア認証だけを使用してPIXとのVPNセッションを確立できます。

0.CSCdx35823

FTP、Telnet、またはWorld Wide Web(HTTP)経由で接続を開始するユーザには、ユーザ名とパスワードの入力が求められます。ユーザ名とパスワードが指定のTACACS+またはRADIUS認証サーバによって確認される場合、PIX Firewallユニットでは、認証サーバと接続の間のそれ以上のトラフィックが、PIX Firewallユニットの「カットスループロキシ」機能を介して独立して対話することを許可します。

TACACS+またはRADIUSを使用した認証のためのHTTPトラフィック要求の処理中に、バッファオーバーフローの脆弱性が原因でPIXがクラッシュしてリロードする場合があります。

『Internetworking Terms and Acronyms』オンラインガイドは、http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htmにあります。『Cisco Systems Terms and Acronyms』オンラインガイドは、http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/cisco12.htmから入手できます。

これらの脆弱性は、Bug ToolkitにBug ID CSCdv83490およびCSCdx35823として文書化されており、2002年11月21日の1600 UTC以降に表示できます。このツールにアクセスするには、登録ユーザであり、ログインしている必要があります。

回避策

これらの脆弱性に対する回避策はありません。Cisco PSIRT では、該当ユーザが修正済みソフトウェア バージョンのコードにアップグレードすることを推奨しています。

修正済みソフトウェア

DDT：説明	修正済みリリース
CSCdv83490:Initial Contact Notify(INITIAL CONTACT NOTIFY)メッセージの処理中に、PIXによってピアとの重複するISAKMP SAが削除されることはありません。	6.0.4以降 6.1.4以降 6.2.1以降
CSCdx35823:TACACS+またはRADIUSを使用してHTTPトラフィック認証を行う際にバッファオーバーフローが発生します。	5.2.9以降

	6.0.4 以降 6.1.4 以降 6.2.2 以降

修正済みソフトウェアバージョンにアップグレードする手順の詳細については、http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htmを参照してください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

これらの脆弱性は、シスコの技術部門およびお客様からPSIRTに報告されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20021120-pix-vulnerability

改訂履歴

リビジョン 1.0	2002年11月20日	初版リリース

利用規約

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。