Cisco PIX Firewall Managerファイルの公開

severity

アドバイザリーID : cisco-sa-19980902-pix-mgr-file

初公開日 : 1998-09-02 17:00

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製品には、PIX Firewall Manager(PFM)と呼ばれる管理アプリケーションが付属しています。PFMはWorldwide-Webベースのアプリケーションで、制限付きのHTTPサーバが含まれています。PFM HTTPサーバはWindows NTコンピュータ上で動作します。PFM HTTPサーバの脆弱性により、サーバに接続できる任意の攻撃者が、Windows NTホストに存在することが事前に判明している任意のファイルを取得できるようになります。ほとんどの場合、これは、ホストがファイアウォールの内側の任意のユーザによる攻撃に対して脆弱であることを意味しますが、ファイアウォールの外側のユーザによる攻撃に対しては脆弱ではありません。

この脆弱性は、Lafayette Life Insurance Companyの企業コンピュータセキュリティマネージャであるBrett M. Oliphantによって発見され、報告されました。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980902-pix-mgr-file で公開されています。

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

4.2(1)以前のPIX Firewallバージョンに付属しているCisco PIX Firewall Manager(PIX FEM)ソフトウェアをWindows NT用に実行しており、信頼できないユーザがPFMサーバのポート8080にTCP接続できる場合は、この脆弱性の影響を受けます。

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

この脆弱性には、Cisco Bug ID CSCdk39378が割り当てられています。

回避策

ソフトウェアの修正が利用可能であるため、シスコは、大多数のお客様にとって最善の対応は、修復されたソフトウェアにアップグレードすることであると考えています。これらの回避策は、通常とは異なる理由でアップグレードできないお客様にのみ提供されます。

多くのお客様がPIX Firewall Manager製品をNTワークステーションにインストールしていますが、PIX Firewallの設定は完了しており、現在はPFMを積極的に使用していません。これらの顧客に対する最も効果的な回避策は、PFMをアンインストールし、必要に応じて後で修復されたバージョンを再インストールすることです。

もう1つの可能な回避策は、PIXファイアウォール自体などのファイアウォールデバイスを使用して、信頼できないユーザがPFMがインストールされているNTホストのポート8080に接続できないようにすることです。お客様の設定によっては、不正な内部ユーザによるアクセスを防ぐために、NTホストをPIX FirewallのDMZネットワークに移動することが望ましい場合があります。この決定を行う際には、DMZネットワーク上の他のシステムのセキュリティを慎重に考慮する必要があります。

PFM HTTPサーバがNTの「administrator」アカウントを使用するのを停止することはできません。

修正済みソフトウェア

この脆弱性は、リリース4.2(1)以前のすべてのCisco PIX Firewall Managerリリースに影響します。4.2(2) betaリリースも影響を受けます。PFMの4.1ベースと4.2ベースの両方のバージョンで修正済みバージョンを使用できます。

4.1の修正バージョンは4.1(6b)です。PFMバージョン4.1(6b)を使用するには、ソフトウェアバージョン4.1(6)をPIX Firewall自体にインストールする必要があります。

4.2の修正済みバージョンは4.2(2)で、PIX Firewall自体の4.2(2)ソフトウェアとともにリリースされる予定です。4.2(1) PIX Firewallソフトウェアは、ソフトウェア品質の問題が原因で回線停止状態にあり、使用またはインストールには推奨されません。したがって、4.2(1) PIX Firewallソフトウェアに対するPFMの修正はありません。4.2(1)をご使用のお客様には、PIX Firewallをバージョ

ン4.1(6)にダウングレードし、PFM 4.1(6b)をインストールすることをお勧めします。これが不可能な場合は、次に示す回避策を使用してください。

これらの修正済みリリースに続くすべてのリリースにも修正が含まれます。今後、脆弱性のあるPFMリリースは存在しません。

不正利用事例と公式発表

シスコには、この脆弱性の悪意のあるエクスプロイトに関する報告はありません。ただし、このような不正利用は近い将来に開始される可能性があります。

この脆弱性の存在は、1998年8月31日（月）に「bugtraq@netspace.org」メーリングリストで公開されました。この脆弱性が存在することは広く知られているものと考えられます。不正利用の詳細は示されていません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980902-pix-mgr-file

改訂履歴

リビジョン 1.0	1998年9月2日	最初にリリースされたバージョン

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。