Common Unix Printing System IPP はメモリ不良脆弱性をタグ付けします

Medium	**アドバイザリーID :** Cisco-SA-20071031-CVE-2007-4351 **初公開日 :** 2007-10-31 17:40 **最終更新日 :** 2012-07-14 19:36 **バージョン 11.0 :** Final **CVSSスコア :** 6.4 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2007-4351

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

Common Unix Printing System （ CUPS ）バージョン 1.3.3 は前に非認証を可能にすることができるサービス拒否 （ DoS ）状態を作成するか、またはユーザの特権と任意のコードを実行するために脆弱性リモート攻撃者が含まれ。

ippReadIO() Â 機能で存在 する脆弱性は Internet Printing Protocol （ IPP ）を処理するときタグ付けします。領域を割り当てるとき Â により機能エラー以外によって 1 引き起こします。Â は非認証、リモート攻撃者ゼロのスタックの 1 バイトを上書きする巧妙に細工されたタグとの要求を送信 する可能性があります。Â は攻撃者デーモンをクラッシュしか、または可能性のある 任意のコードを実行する可能性があります。

ベンダーはリリース ノートおよび releasedÂ のこの脆弱性を更新バージョン確認しました。

脆弱性は攻撃者が不正侵入を行うために IPP TCPポートに接続するように要求します。しかし Â は、CUPS のデフォルト 設定 リモートホストがこのポートに接続しないようにしません。Â はこの設定この不正侵入のための可能性を軽減する必要があります。展開するおよびデフォルト 設定を変更しないで使用 CUPS は危険な状態にないかもしれません Â IT部門。

影響の重大度は展開されるすくうシステムによって変わります。このシステムがマルチプルサービスのために使用されれば Â により、DoS 状態他のユーザおよび部門に影響を与えるかもしれない CUPS サービスのほかのその他のサービスはクラッシュします可能性があります。Â

コード 実行が堪能である場合、CUPS ユーザという点において多分あります。Â はこのユーザおそらく特権を制限しました。

該当製品

CUPS は次のリンクでリリース ノートを提供しました: CUPS 1.3.4

Apple は次のリンクでセキュリティ更新プログラムをリリースしました: セキュリティ更新プログラム 2007-009

Avaya は次のリンクで Security Advisory をリリースしました: ASA-2007-476

Cisco は次のリンクで Cisco バグ ID CSCsl92095 をアドレス指定するためにセキュリティ応答をリリースしました: cisco-sa-20080625-waas

Debian は次のリンクで Security Advisory をリリースしました: DSA-1407-1

FreeBSD は次のリンクで VuXML 文書を発表しました: コップ ---- バッファオーバーフロー以外によって 1

Gentoo は次のリンクで Security Advisory をリリースしました: GLSA 200711-16

Mandriva は次のリンクで Security Advisory をリリースしました: MDKSA-2007:204 および MDKSA-2007:204-1

Red Hat は次のリンクで Security Advisory をリリースしました: RHSA-2007:1020、RHSA-2007:1022 および RHSA-2007:1023

Slackware は次のリンクで Security Advisory をリリースしました: SSA:2007-305-01

SUSE は次のリンクでセキュリティ 発表をリリースしました: SUSE-SA:2007:058

Turbolinux は次のリンクで Security Advisory をリリースしました: TLSA-2008-19

Ubuntu は次のリンクでセキュリティ通知を公開しました: USN-539-1

US-CERT は次のリンクで脆弱性に関する注記を発表しました: VU#446897

脆弱性のある製品

CUPS バージョン 1.3.3 は前に脆弱であり。

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。

回避策

管理者は適切なアップデートを適用するように助言されます。

管理者は信頼されたユーザへのアクセスを制限するように助言されます。

Cisco によって加えられる知性チームは識別を管理者に指示するために次のドキュメントガイドを作成し、軽減は更新済ソフトウェアを加える前にこの脆弱性を不正利用するように試みます: Wide Area Application Services Common Unix Printing System 脆弱性の識別し、軽減不正利用

修正済みソフトウェア

CUPS の更新バージョンは次のリンクで利用できます: CUPS 1.3.4

Apple は次のリンクで更新済ソフトウェアをリリースしました:

セキュリティ更新プログラム 2007-009（ 10.4.11 ユニバーサル ）
セキュリティ更新プログラム 2007-009（ 10.4.11 PPC ）
セキュリティ更新プログラム 2007-009（ 10.5.1 ）

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

Debian は次のリンクで更新済パッケージをリリースしました: Debian

FreeBSD は次のリンクでポート収集更新をリリースします: ポート コレクションインデックス

Gentoo 更新は **出現**コマンドを使用して次のパッケージのために入手することができます: *ネットプリント/コップ*
Mandriva は **MandrivaUpdate** を使用して自動的にアップデートすることができます。

Red Hat パッケージは **up2date** コマンドを使用して更新済である場合もあります。

Slackware パッケージは **upgradepkg** コマンドを使用して更新済である場合もあります。

SUSE は更新済パッケージをリリースしました; ユーザは **YaST** を使用して更新をインストールできます。

Turbolinux パッケージは **turbopkg** コマンドを使用して更新済である場合もあります。

Ubuntu は更新済パッケージをリリースしました; ユーザは**アップデート マネージャ**を使用して更

新をインストールできます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20071031-CVE-2007-4351

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2007-Oct-31

利用規約