Wide Area Application Services(WAAS)Common UNIX Printing System(CUPS)の脆弱性

アドバイザリーID : cisco-sa-20080625-waas
初公開日 : 2008-06-25 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

これは、Common UNIX Printing System(CUPS)の脆弱性に関するセキュリティアドバイザリに対するCisco PSIRTの回答です。CUPSセキュリティアドバイザリは、http://www.cups.org/str.php?L2561で確認できます。

Cisco Wide Area Application Services(WAAS)には、オープンソースのCUPSテクノロジーの統合に基づくプリントサーバが組み込まれており、このCUPSの脆弱性の影響を受けます。

この脆弱性はリモートから不正利用される可能性があり、Cisco WAAS製品で任意のコードが実行される可能性があります。

追加情報

CSCsl92095:IPP値の長さ範囲のチェックが欠落している(STR #2561)

この脆弱性は、CUPSによってSTR #2561として参照されます。このCUPSの脆弱性は、IPP(Internet Printing Protocol)タグを処理する際に、cups/ipp.cの「ippReadIO()」関数で発生する境界エラーによって引き起こされます。攻撃者は、この脆弱性を不正利用して、特別に巧妙に細工された「textWithLanguage」または「nameWithLanguage」タグを含むIPP要求を送信することで、スタック上の1バイトをゼロで上書きする可能性があります。

バージョン4.0.19より前のWAASシステムソフトウェアで使用されているCUPSのバージョンは、WAASで印刷サービスが有効になっている場合、IPPタグの処理におけるこの脆弱性の影響を受けます。

WAASで使用されているシステムソフトウェアのバージョンを確認するには、Graphical User Interface（GUI；グラフィカルユーザインターフェイス）またはCommand Line Interface（CLI；コマンドラインインターフェイス）を使用します。

- WAAS Central ManagerのGUIにログインし、Devices > Devicesの順に選択します。Devicesウィンドウには、リストされている各デバイスのソフトウェアバージョンが表示されます。または、任意のデバイスのコンテンツペインで、Monitoring > Show/Clear Commands > Show Commandsの順に選択します。versionを選択し、Submitをクリックします。セカンダリウィンドウが表示され、show versionコマンドのコマンドラインインターフェイス(CLI)出力が表示されます。

-デバイスにログインし、CLIを使用してコマンドshow versionを入力します。次の例は、4.0.17ビルド14を実行しているデバイスからの出力を示しています。

```
<#root>

waas_lab#

show version

Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2008 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.17 (build b14 Feb 27 2008)
Version: oe7326-4.0.17.14

Compiled 14:42:31 Feb 27 2008 by cnbuild

System was restarted on Thu May 15 16:07:56 2008.
The system has been up for 3 days, 21 hours, 53 minutes, 26 seconds.
```

デフォルトでは、WAAS印刷サービス機能はすべてのWAASデバイスで無効になっています。

印刷サービスが有効になっているかどうかを確認するには、次のいずれかを実行します。

- WAFS EdgeメニューからWAE Device ManagerのGUIにログインして、Configurationを選択します。Print Servicesタブに、Print services enabledのチェックボックスがあります。このチェックボックスをオンにすると、印刷サービスが有効になります。

-デバイスにログインし、CLIを使用してコマンドshow running-config | include print-services enableコマンドを発行します。コマンドからprint-services enableが返された場合は、印刷サービスが有効になっています。次の例は、印刷サービスが有効な場合の出力を示しています。

```
<#root>

waas_lab#

show running-config | include print-services enable
```

```
print-services enable
waas_lab#
```

次の例は、印刷サービスが有効になっていない場合の出力を示しています。

```
<#root>

waas_lab#

show running-config | include print-services enable

waas_lab#
```

このCUPSの脆弱性が不正利用されると、CUPSプロセスはクラッシュし、システムによって自動的に再起動されます。その他のWAAS機能は、アクティブなエクスプロイト時には影響を受けません。

また、不正利用に成功すると、CUPSプロセス権限のみに基づいて任意のコードが実行される可能性があります。

WAASの印刷サービスの詳細については、次のリンクを参照してください。
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/printsvr.html

この脆弱性は、Cisco Bug ID CSCsl92095(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2007-4351が割り当てられています。

ソフトウェア バージョンと修正

ソフトウェアバージョン4.0.19.14以降には、この脆弱性に対する修正が含まれています。このソフトウェアは、http://www.cisco.com/pcgi-bin/tablebuild.pl/waas40?psrtdcat20e2からダウンロードできます。

注：End of Life(EOL)のCisco Wide Area File Services(WAFS)も、この脆弱性の影響を受けます。WAFSの脆弱性は、Cisco Bug ID CSCsl92099(登録ユーザ専用)に記載されています。WAFS用に計画されたソフトウェアリリースはありません。お客様にはWAASへの移行が推奨されます。

回避策

WAASで印刷サービスが不要な場合は、無効にします。WAASの印刷サービスを無効にするには、次のいずれかを実行します。

- WAE Device ManagerのGUIにログインし、WAFS Edgeメニューから Configurationを選択します。Print Servicesタブの下に、Print services enabledのチェックボックスがあります。このチェックボックスがオフになっていることを確認します。

- WAASデバイスにログインし、CLIプロンプトからコンフィギュレーションモードに入り、コマンドno print-services enableを入力します。

ネットワーク内のCiscoデバイスに展開できる追加の緩和テクニックについては、この応答に関連する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-20080625-waas

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080625-waas

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.0	初版リリース		2008年6月25日

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、単独の転載や意訳を施した場合、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。