Cisco Service Control EngineのDoS脆弱性

High

アドバイザリーID : cisco-sa-20080521-sce
初公開日 : 2008-05-21 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2008-0536
CVE-2008-0534
CVE-2008-0535

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 Service Control Engine(SCE)には、システムの不安定性やSCEのリロードを引き起こす可能性のあるSecure Shell(SSH)の脆弱性が3つ存在します。最初の脆弱性は、アグレッシブタイムフレーム内で実行されるSSHログインアクティビティ中にトリガーされる可能性があります。2つ目の脆弱性は、同時に発生する他のSCE管理アクションと組み合わせて、通常のSSHログインアクティビティでトリガーされる可能性があります。3つ目の脆弱性は、SSHログイン中にトリガーされる可能性があり、一意の無効な認証クレデンシャルの使用に固有です。

シスコでは、該当するお客様用に、これらの脆弱性に対応する無償のアップグレードソフトウェアを提供しています。これらの脆弱性に対する回避策はありません。

注：これらの脆弱性は互いに独立しています。デバイスは、他の脆弱性ではなく、1つの脆弱性の影響を受ける可能性があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080521-sce で公開されています。

該当製品

脆弱性のある製品

SCE 1000および2000シリーズデバイスは、SCE上のSSHサーバが有効な場合、次の脆弱性の影響を受けます。

- SSHログインアクティビティに対するシステムの脆弱性：3.1.6より前のSCEソフトウェアバージョンに影響します。
- SSHのログイン操作が不正な入出力操作の原因：3.0.7および3.1.0より前のSCEソフトウェアバージョンに影響します。

- SCE SSH認証シーケンスの異常：3.1.6より前のSCEソフトウェアバージョンに影響します。

注：SCE SSHサーバはデフォルトで無効になっています。

脆弱性のあるバージョンのCisco Service Control Operating System(SCOS)ソフトウェアを実行しているかどうかを確認するには、「Show Version」コマンドラインインターフェイス(CLI)コマンドを発行します。次の例は、ソフトウェアリリース3.1.6が稼働しているCisco SCEを示しています。

```
<#root>

SCE2000#>

show version

System version: Version 3.1.6 Build 157
Build time: Mar 31 2008, 18:58:49 (Change-list 303626)
Software version is: Version 3.1.6 Build 157
```

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 SCE 1000および2000シリーズデバイスは、大容量で高度なアプリケーションレベルの帯域幅最適化、ステートフルアプリケーションインスペクション、セッションベースの分類、およびネットワークトラフィックの制御を提供します。SCEソリューションでは、Webブラウジング、マルチメディアストリーミング、ピアツーピア(P2P)などのネットワークアプリケーションの検出と制御が可能です。

このセキュリティ アドバイザリでは、相互に独立した複数の脆弱性が説明されています。これらの脆弱性は相互に関連していません。

- SSHログインアクティビティに対するシステム脆弱性

SCE SSHサーバに影響を与える脆弱性がSSHログインアクティビティ中にトリガーされ、システムが不安定になったり、SCEのリロードが発生したりする可能性があります。特定のSSHプロセスがアグレッシブな間隔で呼び出されると、一時的なリソースが使用できなくなる場合があります。

この脆弱性は、Cisco Bug ID CSCsi68582(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-2008-0534が割り当てられています。

- SSHログインアクティビティが不正な入出力操作につながる

SCE SSHサーバには、他の管理タスクとともに発生するSCE管理インターフェイスへの通常のSSHトラフィックによってトリガーされる可能性のある2つ目の脆弱性が存在します。このイベントの間、不正なIO操作はSCE管理エージェントに影響を与え、管理アクセスを回復するためにSCEの再起動が必要になる場合があります。

この脆弱性は、Cisco Bug ID CSCsh49563(登録ユーザ専用)として文書化され、CVE ID CVE-2008-0536が割り当てられています。

- SCE SSH認証シーケンスの異常

3つ目の脆弱性はSCE SSHサーバに存在します。この脆弱性はSSHログインプロセス中にもトリガーされる可能性がありますが、ログイン試行回数やその他の同時管理タスクとは無関係です。この問題は、認証方式を変更しようとする特定のSSHクレデンシャルを使用することによって引き起こされ、その結果、認証シーケンスの異常が発生してシステムの安定性に影響を与えます。

この脆弱性は、Cisco Bug ID CSCsm14239(登録ユーザ専用)として文書化され、CVE ID CVE-2008-0535が割り当てられています。

回避策

これらの脆弱性に対する回避策はありません。

SCE管理インターフェイスまたはスクリーニングデバイスで、該当するSCEデバイスへのアクセスコントロールリスト(ACL)を使用してSSHトラフィックをフィルタリングすることにより、これらの脆弱性を緩和できます。SCE ACLまたはトランジットACLを使用して、信頼できるデバイスだけにSCE SSH管理インターフェイスのアクセスを制限することを強くお勧めします。

SCE ACLについての詳細は、SCEソフトウェアコンフィギュレーションガイドの「管理インターフェイスおよびセキュリティの設定」セクションを参照してください。
http://www.cisco.com/en/US/products/ps6134/products_configuration_guide_chapter09186a00808498b9.h

tACLについての詳細は、『トランジットアクセスコントロールリスト：エッジでのフィルタリング』を参照してください。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance

Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

次のリストには、各脆弱性に対する第 1 修正済みソフトウェア リリースが含まれています。

脆弱性	該当するメジャーリリース	First Fixed Release（修正された最初のリリース）
SSHログインアクティビティに対するシステム脆弱性	1.x	3.1.6
	2.x	3.1.6
	3.x	3.1.6
SSHログインアクティビティが不正なIO操作につながる	1.x	3.0.7
	2.x	3.0.7
	3.x	3.0.7, 3.1.0
SCE SSH認証シーケンスの異常	1.x	3.1.6
	2.x	3.1.6
	3.x	3.1.6

SCOSソフトウェアバージョン3.1.6には、このドキュメントで説明されているすべての脆弱性に対する修正が含まれています。

SCOSソフトウェアは、cisco.comの次の場所からダウンロードできます。

- SCOS 3.1.6(登録ユーザのみ)

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公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

SSHログインアクティビティの脆弱性は、カスタマーサポートケースの解決中に発見されました。

不正な入出力動作と認証シーケンスの異常は、シスコの社内テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080521-sce

改訂履歴

リビジョン 1.0	2008年5月21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。