Cisco IOS XRソフトウェアのSSHにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20100120-xr-ssh

初公開日 : 2010-01-20 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-2010-0137

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 IOS XRソフトウェアのSSHサーバの実装には、認証されていないリモートユーザが不正利用してサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が含まれています。

攻撃者は、新しいSSH接続ハンドラプロセスをクラッシュさせる可能性のある巧妙に細工されたSSHバージョン2パケットを送信することにより、この脆弱性を引き起こす可能性があります。この脆弱性が繰り返し悪用されると、新しいSSH接続ハンドラプロセスがクラッシュし、大量のメモリが消費される結果、他のシステム機能に悪影響を及ぼす不安定性が発生する可能性があります。このイベントの間、親SSHデーモンプロセスは正常に機能し続けます。

シスコはこ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-20100120-xr-ssh で公開されています。

該当製品

脆弱性のある製品

この脆弱性は、該当バージョンのCisco IOS XRソフトウェアを実行し、SSHサーバ機能が有効になっているCisco IOS XRシステムに影響を与えます。SSHサーバ機能が有効になっているシステムの設定には、**ssh server [v2]**コマンドが含まれています。Cisco IOS XRソフトウェアでのSSHサーバの設定に関する詳細については、『Cisco IOS XR System Security Configuration

Guide』(http://www.cisco.com/en/US/docs/routers/crs/software/crs_r3.9/security/configuration/guide/sc39ssh.html#wp1044523)を参照してください。

SSHサーバは、「security」パッケージ情報エンベロープ(PIE)がインストールされている場合にのみ、Cisco IOS XRソフトウェアで有効にできます。管理者は**show install summary**コマンドを発行して、セキュリティPIEがインストールされているかどうかを確認できます。このコマンドを実行すると、「<platform>-k9sec-<version>」のようなアクティブなパッケージが表示されます。たとえば、セキュリティPIEがインストールされている場合は、「c12k-k9sec-3.6.1」のように表示されます。

影響を受ける特定のソフトウェアバージョンの詳細については、このアドバイザリの「ソフトウェアバージョンと修正」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアにおけるSSHサーバの実装は、この脆弱性の影響を受けません。

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 IOS XRソフトウェアは、マイクロカーネルベースの分散オペレーティングシステムインフラストラクチャを使用するCisco IOSソフトウェアファミリのメンバーです。Cisco IOS XRソフトウェアは、Cisco CRS-1キャリアルーティングシステム、Cisco 12000シリーズルータ、およびCisco ASR 9000シリーズアグリゲーションサービスルータで動作します。Cisco IOS XRソフトウェアの詳細については、http://www.cisco.com/en/US/products/ps5845/index.htmlを参照してください。

SSHプロトコルは、Telnet、FTP、rlogin、リモートシェル(rsh)、およびリモートコピープロトコル(RCP)プロトコルに代わる安全なプロトコルとして開発され、リモートデバイスへのアクセスを可能にします。SSHは、強力な認証と機密性を提供し、暗号化されたトランザクションを使用するという点で、これらの古いプロトコルとは異なります。

Cisco IOS XRソフトウェアのSSHサーバの実装には、認証されていないリモートユーザが不正利用してサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が含まれています。

この脆弱性は、新しいSSHハンドラプロセスが巧妙に細工されたSSHバージョン2パケットを処理し、プロセスがクラッシュする可能性がある場合にトリガーされます。このイベントの間、大量のメモリが消費される可能性があります。この脆弱性が繰り返し悪用されると、使用可能なメモリのサイズと攻撃期間によっては、他のシステム機能に影響を与える可能性があります。

この脆弱性の不正利用にはユーザ認証は必要ありませんが、TCP 3ウェイハンドシェイクを完了し、SSHプロトコルネゴシエーションを実行する必要があります。

SSHサービスは、攻撃中および攻撃後も正常に機能し続けます。

この脆弱性のエクスプロイト時に、システムは次のメッセージを生成する可能性があります。

```
RP/0/RP1/CPU0:Jan 14 16:56:34.885 : dumper[59]: %OS-DUMPER-7-DUMP_ATTRIBUTE :
     Dump request with attribute 407 for process pkg/bin/sshd_child_handler
RP/0/RP1/CPU0:Jan 14 16:56:34.897 : dumper[59]: %OS-DUMPER-7-SIGSEGV :
     Thread 1 received SIGSEGV
RP/0/RP1/CPU0:Jan 14 16:56:34.901 : dumper[59]: %OS-DUMPER-7-BUS_ADRERR :
     Accessed BadAddr 50199000 at PC 4a280c64
RP/0/RP1/CPU0:Jan 14 16:56:34.906 : dumper[59]: %OS-DUMPER-4-CRASH_INFO :
     Crashed pid = 21733716 (pkg/bin/sshd_child_handler)
```

この脆弱性は、Cisco Bug ID **CSCsu10574** (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-2010-0137が割り当てられています。

回避策

この脆弱性に対する回避策はありません。ネットワーク管理者は、脆弱性の影響を抑えるために緩和策を適用することを推奨します。緩和策には、正当なデバイスだけがルータに接続できるようにする方法があります。

これらのアクセス制限は、インターフェイスアクセスコントロールリスト(ACL)またはCisco IOS XRソフトウェアリリース3.5以降で使用可能な管理プレーン保護(MPP)機能を使用して実現できます。MPPの詳細については、
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.8/security/configuration/guide/sc38mpp.html
にあるコンフィギュレーションガイドと
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.8/security/command/reference/sr38mpp.html
にあるMPPコマンドリファレンスを参照してください。インフラストラクチャACL(iACL)も、この脆弱性の潜在的な不正利用を軽減するための有用な手法です。

これらの緩和策の詳細については、
http://www.cisco.com/web/about/security/intelligence/CiscoIOSXR.htmlにある『Cisco Guide to Harden Cisco IOS XR Devices』を参照してください。

VTYプールに適用される回線テンプレート内のアクセスクラスは、この脆弱性に対する効果的な緩和策ではないことに注意してください。

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。

この脆弱性は、次の表に従って適切なSoftware Maintenance Upgrade(SMU)を適用することで対処できます。適切なSMUのインストールでは、システムのリロードは必要ありません。Cisco IOS XRソフトウェアおよびSMUの詳細については、ドキュメント『Guidelines for Cisco IOS XR Software』(http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product_bulletin_c25-478699.html)を参照してください。

Cisco IOS XRリリース	SMU名およびSMU ID		
	CRS-1	XR12000	ASR 9000 (*)
3.4.1	hfr-k9sec-3.4.1.CSCsu10574AA03509	c12k-k9sec-3.4.1.CSCsu10574AA03532	該当なし
3.4.2	hfr-k9sec-3.4.2.CSCsu10574AA03510	c12k-k9sec-3.4.2.CSCsu10574AA03531	該当なし
3.4.3	hfr-k9sec-3.4.3.CSCsu10574AA03511	c12k-k9sec-3.4.3.CSCsu10574AA03530	該当なし
3.5.2	hfr-k9sec-3.5.2.CSCsu10574AA03512	c12k-k9sec-3.5.2.CSCsu10574AA03529	該当なし
3.5.3	hfr-k9sec-3.5.3.CSCsu10574AA03513	c12k-k9sec-3.5.3.CSCsu10574AA03528	該当なし
3.5.4	hfr-k9sec-3.5.4.CSCsu10574AA03514	c12k-k9sec-3.5.4.CSCsu10574AA03527	該当なし
3.6.0	hfr-k9sec-3.6.0.CSCsu10574AA03515	c12k-k9sec-3.6.0.CSCsu10574AA03526	該当なし
3.6.1	hfr-k9sec-3.6.1.CSCsu10574AA03516	c12k-k9sec-3.6.1.CSCsu10574AA03525	該当なし
3.6.2	Not affected	Not affected	該当なし
3.6.3	Not affected	Not affected	該当なし
3.7.0	hfr-k9sec-3.7.0.CSCsu10574AA03519	c12k-k9sec-3.7.0.CSCsu10574AA03522	該当なし

3.7.1	Not affected	Not affected	Not affected
3.7.2	Not affected	Not affected	Not affected
3.8.x	Not affected	Not affected	該当なし
3.9.x	Not affected	Not affected	Not affected

(*)Cisco ASR 9000アグリゲーションサービスルータでは、すべてのCisco IOS XRソフトウェアバージョンがサポートされているわけではありません。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、Cisco の社内テストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100120-xr-ssh

改訂履歴

リビジョン 1.0	2010年1月20日	初版リリース

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。