Cisco IOS XR ソフトウェア ルートプロセッサ サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20120530-iosxr

初公開日 : 2012-05-30 16:00

最終更新日 : 2012-08-23 20:37

バージョン 2.1 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCtz62593 CSCty94537 CSCua63591

CVE-2012-2488

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 ソフトウェアはサービス拒否状態という結果に終るかもしれない巧妙に細工されたパケットを処理するとき脆弱性が含まれています。 on Cisco 9000 シリーズ集約を存在 するただ脆弱性はルータ（ASR）Route Switch Processor（RSP-4G および RSP-8G）、Route Switch Processor 440（RSP440）、および Cisco Carrier Routing System（CRS）Performance Route Processor（PRP）を保守します。 脆弱性は巧妙に細工されたパケットの不適当な処理の結果で、ファブリックにパケットを送信することがパケットを処理するルートプロセッサを引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120530-iosxr

該当製品

この脆弱性は Cisco ASR 9000 シリーズ RSP-4G か RSP-8G で動作する 4.2.0 前に Cisco ASR 9000 シリーズ RSP440 および IOS XR ソフトウェア バージョンで動作する IOS XR ソフトウェア バージョン 4.2.0 に影響を与えます。 それはまた CRS Performance Route Processor で動作する IOS XR ソフトウェア バージョン 4.0.3、4.0.4、4.1.0、4.1.1、4.1.2、および 4.2.0 に影響を与えます。

脆弱性のある製品

Cisco IOS XR ソフトウェアを Cisco製品で動作している、管理者できますログイン判別し、システムバナーを表示する **show version コマンドを**発行することはデバイスにリリースします。 システムバナーはデバイスが「Cisco IOS XR ソフトウェアと」ことを同じようなテキストの表示によって Cisco IOS XR ソフトウェアを実行していることを確認します。 ソフトウェアバージョンはテキスト「Cisco IOS XR ソフトウェア」の後で表示されます。

次の例は Cisco IOS XR ソフトウェア リリース 4.2.0 を実行している Cisco ASR 9000 シリーズ デバイスを識別したものです:

```
RP/0/RSP1/CPU0:ASR9006-D#show version | inc Cisco IOS XR Software
Fri Apr 27 22:40:32.486 UTC
Cisco IOS XR Software, Version 4.2.0[Default]
```

次の例は Cisco IOS XR ソフトウェア リリース 4.0.4 を実行している Cisco CRS シリーズ デバイスを識別したものです:

```
RP/0/RP0/CPU0:CRS-G#show version | inc Cisco IOS XR Software
Fri Apr 27 22:28:14.304 UTC
Cisco IOS XR Software, Version 4.0.4[Default]
```

Cisco IOS XR ソフトウェア リリース命名規則についてのその他の情報は「白書で利用できます: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/web/about/security/intelligence/ios-ref.html#9

Cisco IOS XR ソフトウェア時間ベース リリースモデルについてのその他の情報は「白書で利用できます: 次のリンクの Cisco IOS XR ソフトウェアのためのガイドライン」: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8803/ps5845/product_bulletin_c25-478699.html

影響を受けたソフトウェアが付いている Cisco ASR 9000 シリーズ デバイスが RSP440 を使用しているかどうか判別するために、次のコマンドは実行することができます:

```
RP/0/RSP0/CPU0:ASR9006-D#show inventory all | include Route Switch Processor
Thu May  3 18:50:46.129 UTC
NAME: "module 0/RSP0/CPU0", DESCR: "ASR9K Route Switch Processor with 440G/slot Fabric and
6GB"
NAME: "module 0/RSP1/CPU0", DESCR: "ASR9K Route Switch Processor with 440G/slot Fabric and
6GB"
```

パフォーマンス ルートプロセッサが装備されているデバイスだけ影響を受けています。 影響を受けたソフトウェアが付いている Cisco CRS シリーズ デバイスが Performance Route Processor を使用しているかどうか判別するために、次のコマンドは実行することができます:

```
RP/0/RP0/CPU0:CRS-G#show inventory all | include Performance Route Processor
Wed May  2 14:49:06.994 EDT
NAME: "0/RP0/*", DESCR: "Cisco CRS Series 8 Slots 12 GB Performance Route Processor"
NAME: "0/RP1/*", DESCR: "Cisco CRS Series 8 Slots 12 GB Performance Route Processor"
```

脆弱性を含んでいないことが確認された製品

Cisco ASR 9000 シリーズだけ RSP440、RSP-4G および RSP-8G デバイスおよび Cisco

Carrier Routing System Performance Route Processor デバイスは影響を受けています。

その他のCisco製品は現在 Cisco CRS-1 分散ルートプロセッサ（DRP）、RP-A または RP-B のような他のルートプロセッサを含むこの脆弱性から、影響を受けるために知られていません。

詳細

Cisco IOS XR ソフトウェアは特定の設定の 2 つの異なるプラットフォームにあるこの脆弱性から影響を受けます。

脆弱なソフトウェア バージョンは次のいずれかのルートプロセッサと影響を受けるために結合する必要があります:

プラットフォーム	ルートプロセッサ部品 ID
ASR 9000	A9K-RSP440-SE
ASR 9000	A9K-RSP440-TR
ASR 9000	A9K-RSP-4G
ASR 9000	A9K-RSP-8G
CRS	CRS-8-PRP-6G
CRS	CRS-8-PRP-12G
CRS	CRS-16-PRP-6G
CRS	CRS-16-PRP-12G

この脆弱性は Cisco バグ ID CSCty94537 および CSCua63591 で文書化されています（ASR 9000）および CSCtz62593（CRS は）およびよくある脆弱性および公開（CVE） ID CVE-2012-2488 は割り当てられました。

Cisco IOS XR ソフトウェア ルートプロセッサ サービス拒否の脆弱性

Cisco IOS XR ソフトウェアにより非認証を可能にする可能性があるサービス拒否（DoS）状態を引き起こすために脆弱性がリモート攻撃者含まれています。

脆弱性は Cisco 9000 シリーズ集約サービス ルータ（ASR） Route Switch Processor（RSP-4G か RSP-8G）、Route Switch Processor 440（RSP440）、Cisco CRS 16 スロット ラインカード シャーシ ルートプロセッサ B（RP-B）、または Carrier Routing System（CRS） Performance Route Processor によって巧妙に細工されたパケットの不適当な処理が原因です。 攻撃者は脆弱なシステムへ巧妙に細工されたパケットを送信 することによってこの脆弱性を不正利用する可能性があります; この脆弱性は脆弱なデバイスを通過する IP トラフィックによって引き起こすことができません。 エクスプロイトは攻撃者により DoS 状態に終ってファブリックに、送信することを止めるためにルートプロセッサ CPU で起きるパケットを引き起こすことを可能にする可能性があります。

回避策

この文書に説明がある脆弱性のための回避策がありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、 http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

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。

ASR 9000 シリーズ RSP440 を on Cisco 実行する IOS XR に関しては脆弱性はソフトウェア バージョン 4.2.0 にあり、SMU 名前 4.2.0_asr9k-px_REC_SMUS_2012-05-15.tar と固定されます。

ASR 9000 シリーズ RSP-4G か RSP-8G を on Cisco 実行する IOS XR に関しては脆弱性は 4.2.0 前にバージョンにあります。 ASR 9000 シリーズ RSP-4G 用の次の SMUs か RSP-8G デバイスはこの脆弱性を解決します:

IOS XR バージョン	SMU ID	SMU 名
4.0.1	AA06294	asr9k-p-4.0.1.CSCua63591
4.0.3	AA06313	asr9k-p-4.0.3.CSCua63591
4.1.0	AA06306	asr9k-p-4.1.0.CSCua63591
4.1.1	AA06308	asr9k-p-4.1.1.CSCua63591
4.1.2	AA06305	asr9k-p-4.1.2.CSCua63591

CRS Performance Route Processor で動作する IOS XR に関しては脆弱性はバージョン 4.0.3、4.0.4、4.1.0、4.1.1、4.1.2、および 4.2.0 にあります。 CRS シリーズ デバイスのための次の SMUs はこの脆弱性を解決します:

IOS XR バージョン	SMU ID	SMU 名
4.0.3	AA06162	hfr-px-4.0.3.CSCtz62593
4.0.4	AA06161	hfr-px-4.0.4.CSCtz62593
4.1.0	AA06163	hfr-px-4.1.0.CSCtz62593
4.1.1	AA06164	hfr-px-4.1.1.CSCtz62593
4.1.2	AA06165	hfr-px-4.1.2.CSCtz62593
4.2.0	AA06166	hfr-px-4.2.0.CSCtz62593

この脆弱性は Cisco 両方 ASR 9000 シリーズ デバイスおよび CRS シリーズ デバイスのための IOS XR バージョン 4.2.1 で解決されます。

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。

この脆弱性はカスタマ ネットワークで見つけられた問題を診断している間検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120530-iosxr

改訂履歴

Revision 2.1	2012-August-23	最初公開日を訂正するためにアップデートされるドキュメント
Revision 2.0	2012-August-15	IOS XR 4.2.0 前に ASR 9000 シリーズの RSP-4G および RSP-8G が、含まれる更新済影響を受けたプラットフォーム
リビジョン 1.1	2012-May-31	SMU 名前を明白にし、関連したソフトウェアダウンロード ページへのリンクを提供する更新済ソフトウェア バージョン および 修正
リビジョン 1.0	2012-May-30	初版リリース

利用規約