

Cisco IOS XR ソフトウェア Border Gateway Protocol (BGP) 脆弱性

Medium	アドバイザーID : cisco-sa-20090818-bgp	CVE-2009-1154
m	初公開日 : 2009-08-18 15:00	CVE-2009-2055
	バージョン 2.6 : Final	CVE-2009-2055
	CVSSスコア : 4.3	CVE-2009-2056
	回避策 : Yes	
	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

Cisco IOS XR ソフトウェアはボーダー ゲートウェイ プロトコル (BGP) 機能で多重脆弱点が含まれています。これには次のバージョンが含まれます。

- Cisco IOS XR ソフトウェアは特定の無効な BGP更新を受信するとき BGP ピアリングセッションを再設定します。
脆弱性は BGPピアが特定の無効な アトリビュートのプレフィクスをアナウンスすると明示します。このプレフィクスの受信で、Cisco IOS XR デバイスは通知の送信によってピアリングセッションを再始動します。ピアリングセッションは送信側が無効な/破損 アップデートを送信することを止めるまでフラップします。この脆弱性はこのアドバイザーの Revision 1.0 で表われました。
- Cisco IOS XR BGPプロセスは長い長さ BGP更新 メッセージを送信するときクラッシュします
Cisco IOS XR が長い長さ BGP更新 メッセージを送信するとき、BGPプロセスはクラッシュするかもしれません。実稼働環境の内で見られる正常な制限の上にアップデートメッセージの合計/最大長を超過し、クラッシュを引き起こすために必要な AS 数の数がよくあります。
- Cisco IOS XR BGPプロセスは多数の AS の BGP更新を組み立てるとき付加するクラッシュします
AS パスに非常に多くの自律 システム (AS) 数を付加するために Cisco IOS XR BGPプロセスが設定される場合 BGPプロセスはクラッシュします。実稼働環境の内で見られる正常な制限の上に付加されるために必要な AS 数の数によりクラッシュをよくあります引き起こし。

3 脆弱性はすべて次のリンクの 1600 UTC Border Gateway Protocol (BGP) 表われたものからの 2009 年 July 29 の Cisco Security Advisory 「Cisco IOSソフトウェア 4 バイト 自律システム番号脆弱性」で異なる脆弱性です:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090729-bgp>。

Cisco はフリーソフト メンテナンスアップデート (SMU) をそのアドレスこれらの脆弱性リリースしました。

回避策はこれらの脆弱性を軽減する利用できます。

このアドバイザリは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090818-bgp> で掲示されます

該当製品

修正済みソフトウェア

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を表示するによって 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」の後で表示する。

Cisco IOS XR ソフトウェア リリース 3.6.2 を実行している次の例は Cisco CRS-1 を識別したものです:

```
RP/0/RP0/CPU0:CRS#show version
Tue Aug 18 14:25:17.407 AEST

Cisco IOS XR Software, Version 3.6.2[00]
Copyright (c) 2008 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 1.49(20080319:195807) [CRS-1 ROMMON],

CRS uptime is 4 weeks, 4 days, 1 minute
System image file is "disk0:hfr-os-mbi-3.6.2/mbihfr-rp.vm"

cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revision 1.2

17 Packet over SONET/SDH network interface(s)
1 DWDM controller(s)
17 SONET/SDH Port controller(s)
8 TenGigabitEthernet/IEEE 802.3 interface(s)
2 Ethernet/IEEE 802.3 interface(s)
1019k bytes of non-volatile configuration memory.
38079M bytes of hard disk.
981440k bytes of ATA PCMCIA card at disk 0 (Sector size 512 bytes).

Configuration register on node 0/0/CPU0 is 0x102
```

Boot device on node 0/0/CPU0 is mem:

!--- output truncated

次の例は Cisco IOS XR ソフトウェア リリース 3.7.1 を実行している Cisco 12404 ルータを識別したものです:

```
RP/0/0/CPU0:GSR#show version
```

```
Cisco IOS XR Software, Version 3.7.1[00]  
Copyright (c) 2008 by Cisco Systems, Inc.
```

```
ROM: System Bootstrap, Version 12.0(20051020:160303) SOFTWARE  
Copyright (c) 1994-2005 by cisco Systems, Inc.
```

```
GSR uptime is 3 weeks, 6 days, 3 hours, 20 minutes  
System image file is "disk0:c12k-os-mpi-3.7.1/mbiprp-rp.vm"
```

```
cisco 12404/PRP (7457) processor with 2097152K bytes of memory.  
7457 processor at 1266Mhz, Revision 1.2
```

```
1 Cisco 12000 Series Performance Route Processor  
1 Cisco 12000 Series - Multi-Service Blade Controller  
1 1 Port ISE Packet Over SONET OC-48c/STM-16 Controller (1 POS)  
1 Cisco 12000 Series SPA Interface Processor-601/501/401  
3 Ethernet/IEEE 802.3 interface(s)  
1 SONET/SDH Port controller(s)  
1 Packet over SONET/SDH network interface(s)  
4 PLIM QoS controller(s)  
8 FastEthernet/IEEE 802.3 interface(s)  
1016k bytes of non-volatile configuration memory.  
1000496k bytes of disk0: (Sector size 512 bytes).  
65536k bytes of Flash internal SIMM (Sector size 256k).
```

```
Configuration register on node 0/0/CPU0 is 0x2102  
Boot device on node 0/0/CPU0 is disk0:
```

!--- output truncated

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「白書で利用できません: Cisco IOS Reference Guide」で確認できます:

<http://www.cisco.com/warp/public/620/1.html#t6>。

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。

BGP は設定コマンド **ルータ BGP [AS 数]**または**ルータ BGP [X.Y]**で Cisco IOS XR ソフトウェアで設定されます。デバイスは影響を受けた Cisco IOS XR ソフトウェア バージョンを実行して、BGP を設定してもらえば脆弱です。

次の例は BGP で設定される Cisco IOS XR ソフトウェア デバイスを示したものです:

```
RP/0/0/CPU0:GSR#show running-config | begin router bgp  
Building configuration...  
router bgp 65535  
  bgp router-id 192.168.0.1
```

```
address-family ipv4 unicast
network 192.168.1.1/32
!
address-family vpv4 unicast
!
neighbor 192.168.2.1
remote-as 65534
update-source Loopback0
address-family ipv4 unicast
!
```

!--- output truncated

脆弱性を含んでいないことが確認された製品

以下のシスコ製品は確認された脆弱です:

- Cisco IOS ソフトウェア
- BGP ルーティングのために設定されない Cisco IOS XR ソフトウェア

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。

改訂履歴

Revision 2.6	2009-August-27	ソフトウェア テーブルへのマイナーな修正
Revision 2.5	2009-August-24	ソフトウェア テーブルへの追加された最終的な SMUs。
Revision 2.4	2009-August-23	ソフトウェア テーブルへの最近追加された利用可能な SMUs。
Revision 2.3	2009-August-22	ソフトウェア テーブルへの最近追加された利用可能な SMUs。
Revision 2.2	2009-August-21	ソフトウェア テーブルへの最近追加された利用可能な SMUs。
Revision 2.1	2009-August-20	ソフトウェア テーブルおよび別々 CVSS 表への追加された現在利用できる SMUs。
Revision 2.0	2009-August-20	傘修正にすべてのバグを含める主要なアップデート。
リリース 1.0	2009-August-18	初回公開リリース

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、単独の転載や意識を施した場合、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。