Cisco IOSソフトウェア IPsec 脆弱性

High

アドバイザリーID : cisco-sa-20100324-ipsec
初公開日 : 2010-03-24 16:00
最終更新日 : 2012-09-21 19:08
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : Yes
Cisco バグ ID : CSCtb13491

CVE-2010-0578

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

不正 な インターネット キー エクスチェンジ（IKE）パケットによりリロードするために Cisco IOSソフトウェアを実行するデバイスを引き起こすかもしれません。 インストールされる VPN Acceleration モジュール 2+（VAM2+）と Cisco IOSソフトウェアを実行している Cisco 7200 シリーズだけおよび Cisco 7301 ルータは影響を受けています。 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ました。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-ipsec で掲示されます。

注: 2010 年 3月 24 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 7 つのセキュリティ アドバイザリが含まれています。 すべてのアドバイザリは Cisco IOSソフトウェアの脆弱性に対処します。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。 次の URLリストの表は正しい 2010 年 3月 24 日送達されたすべての Cisco IOSソフトウェア脆弱性、またはそれ以前ことリリースします:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-bundle

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar10.html

該当製品

修正済みソフトウェア

VPN Acceleration モジュール 2+（VAM2+）の Cisco 7200 シリーズだけおよび Cisco 7301 ルータはこの脆弱性から影響を受けます。

暗号化エンジンのための構成情報の要約を表示する、VAM がおよびデバイスで使用されてあったかどうか確認するために、次の例に示すように **show crypto engine brief** コマンドを、使用して下さい:

```
Router#show crypto engine brief
        crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
                  Location:  slot 4
        VPN Module in slot:  4
              Product Name:  VAM2+
         Software Serial #:  55AA
                 Device ID:  001F - revision 0000
                 Vendor ID:  0000
                Revision No:  0x001F0000
              VSK revision:  0
              Boot version:  902
               DPU version:  0
               HSP version:  3.4(3) (PRODUCTION)
              Time running:  00:00:10
               Compression:  Yes
                       DES:  Yes
                     3 DES:  Yes
                   AES CBC:  Yes (128,192,256)
                  AES CNTR:  No
     Maximum buffer length:  4096
          Maximum DH index:  5120
          Maximum SA index:  5120
        Maximum Flow index:  10230
```

注: 前例では、インストールされるルータに VAM2+ があることを示す「製品名」**VAM2+ は**表示する。「状態」の下の **Enabled キーワードは** VAM2+ がアクティブ 有効に なることを示し。

IKE は IPsec が使用される場合デフォルトで有効に なります。 IKE のために設定される Cisco IOSデバイスは UDP ポート 500、UDP ポート 4500、または UDP ポート 848 または 4848 でデバイスがグループ ドメイン オブ インタープリテーション（GDOI）のために設定される場合デバイスが NAT 走査（NAT-T）のために設定されれば受信します。 UDP ポート 500 で受信しているルータを以下に示します:

```
    Router#show ip sockets
    Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
    ....
     17   --listen--          192.168.66.129    500   0   0   11   0
    ....
```

Or

```
    Router#show udp
    Proto        Remote      Port      Local       Port  In Out  Stat TTY OutputIF
```

```
 17       --listen--          192.0.2.1         500   0   0  1011   0
 17(v6)   --listen--          --any--           500   0   0 20011   0
Router#
```

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
....
 17   --listen--          192.168.66.129    500   0   0   11   0
....
```

Or

```
Router#show udp
Proto        Remote      Port      Local       Port  In Out  Stat TTY OutputIF
 17       --listen--          192.0.2.1         500   0   0  1011   0
 17(v6)   --listen--          --any--           500   0   0 20011   0
Router#
```

次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T を実行している Cisco製品を指定したものです:

```
Router#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
....
 17   --listen--          192.168.66.129    500   0   0   11   0
....
```

Or

```
Router#show udp
Proto        Remote      Port      Local       Port  In Out  Stat TTY OutputIF
 17       --listen--          192.0.2.1         500   0   0  1011   0
 17(v6)   --listen--          --any--           500   0   0 20011   0
Router#
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます:
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性を含んでいないことが確認された製品

Cisco IOS XE および Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。 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。

改訂履歴

リビジョン 1.0	2010-March-24	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。