Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and Cisco ASA

目次

要約

Cisco ASA 5500 シリーズ 適応型セキュリティアプライアンスおよび Cisco PIX セキュリティアプライアンスに複数の脆弱性が存在しています。このアドバイザリは以下の脆弱性の要点について説明しています。

- Crafted TCP ACK Packet Vulnerability
- Crafted TLS Packet Vulnerability
- Instant Messenger Inspection Vulnerability
- Vulnerability Scan Denial of Service
- Control-plane Access Control List Vulnerability

最初の 4 つの脆弱性はサービス妨害(DoS: Denial of Service)攻撃につながる可能性があり、5 つ目の脆弱性は攻撃者にコントロールプレーンアクセスリスト(ACL)をバイパスされる可能性があります。

注: これらの脆弱性についてはそれぞれ独立したものであり、ある機器が 1 つの脆弱性の影響を受け、他の脆弱性の影響は受けない場合もあります。

Ciscoはこれらの脆弱性対応用の無償ソフトウェアを提供しています。
また、この中のいくつかの脆弱性には影響を軽減する回避策が存在します。

本アドバイザリは右記にて確認可能です。
http://www.cisco.com/en/US/products/products_security_advisory09186a00809a8354.shtml.

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。

該当製品

脆弱性のある製品

以下に本アドバザリの各脆弱性の詳細について示します。

Crafted TCP ACK Packet Vulnerability

7.1(2)70 より前の 7.1x、7.2(4) より前の 7.2.x、8.0(3)10 より前の 8.0.xソフトウェアバージョンが稼動しているCisco ASA 及び PIX は本脆弱性の影響を受けます。ソフトウェアバージョン 7.0.xや 8.1.x のCisco ASA 及び PIX セキュリティ アプライアンスは本脆弱性の影響を受けません。

ソフトウェアバージョン7.1.x や7.2.xが稼動するCisco ASA 及び PIX は、WebVPN, SSL VPN, や ASDMが有効な場合に本脆弱性の影響を受けます。ソフトウェアバージョン8.0が稼動するCisco ASA 及び PIX は、Telnet, Secure Shell (SSH), WebVPN, SSL VPN や ASDMが有効な場合に本脆弱性の影響を受けます。

注: IPv4が動作する場合にもIPv6が動作する場合にも本脆弱性は存在します。

Crafted TLS Packet Vulnerability

8.0(3)9 より前の8.0.x、8.1(1)1より前の8.1.x ソフトウェアバージョンが稼動しているCisco ASA 及び PIX 上で HTTPS サーバが有効になっている場合に、本脆弱性の影響を受けます。7.x ソフトウェアバージョンの稼動している Cisco ASA及び PIX は本脆弱性の影響を受けません。

Instant Messenger Inspection Vulnerability

7.2(4) より前の 7.2.x、8.0(3)10 より前の 8.0.x、あるいは8.1(1)2 より前の 8.1.x ソフトウェアバージョンが稼動し、Instant Messaging Inspectionが有効となっているCisco ASA 及び PIX は本脆弱性の影響を受けます。7.0.x 及び 7.1.x ソフトウェアバージョンが稼動する機器は本脆弱性の影響を受けません。また、Instant Messaging Inspectionが有効となっていない機器は本脆弱性の影響を受けません。

注: Instant Messaging Inspectionはデフォルトで無効とされています。

Vulnerability Scan Denial of Service

7.2(3)2 より前の 7.2.x、8.0(2)17 より前の 8.0.x ソフトウェアバージョンが稼動するCisco ASA 及び PIX は本脆弱性の影響を受けます。7.0.x、7.1.x、あるいは 8.1.x ソフトウェアバージョンが稼動する機器は本脆弱性の影響を受けません。

Control-plane Access Control List Vulnerability

8.0(3)9 より前の 8.0.x ソフトウェアバージョンが稼動し、control-plane ACL が設定されている Cisco ASA 及び PIX は本脆弱性の影響を受けます。7.x、あるいは 8.1.x ソフトウェアバージョンが稼動する機器は本脆弱性の影響を受けません。

注: Control-plane ACLはソフトウェアバージョン8.0(2)で導入されました。Control-plane ACLはデフォルトで無効とされています。

show version CLIコマンドによりCisco ASA 及び PIX のソフトウェアバージョンを確認することが出来ます。以下の例は、ASA セキュリティ アプライアンスでソフトウェアバージョン 8.0(2) が稼動していることを示しています。

```
ASA# show version

Cisco Adaptive Security Appliance Software Version 8.0(2)
Device Manager Version 6.0(1)

[...]
```

Cisco Adaptive Security Device Manager (ASDM)を使用して機器を管理している場合には、ログイン ウィンドウのテーブル、あるいはASDMウィンドウの左上のコーナーにソフトウェアバージョンが表示されます。

脆弱性が存在しない製品

Cisco Firewall Services Module (FWSM) は上記脆弱性の影響を受けません。
ソフトウェアバージョン 6.x が稼動するCisco PIX セキュリティ アプライアンスは上記脆弱性の影響を受けません。これ以外のCisco製品において本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

本セキュリティアドバイザリは、複数の異なる脆弱性を記述します。これらの脆弱性は、互いに独立しています。

1. Crafted TCP ACK Packet Vulnerability

巧妙に細工されたTCP ACKパケットによって、Cisco ASA 及び PIX アプライアンスは、サービス妨害を引き起こされる可能性があります。本脆弱性はこのパケットが機器を宛先とする場合のみ影響します。機器を通過する場合は本脆弱性の影響を受けません。

ソフトウェアバージョン7.1.x や7.2.x が稼動するCisco ASA 及び PIX は、WebVPN, SSL VPN や ASDMが有効の場合に本脆弱性の影響を受けます。ソフトウェアバージョン8.0が稼動するCisco ASA 及び PIX は、Telnet, Secure Shell (SSH), WebVPN, SSL VPN や ASDMが有効の場合に本脆弱性の影響を受けます。

telnet コマンドはセキュリティ アプライアンスへの Telnet 接続が許可されるIP アドレスを設定するために用いられます。

```
ASA(config)# telnet 192.168.10.0 255.255.255.0 inside
```

上記の設定例はCisco ASA の inside インタフェースに対して IP アドレス192.168.10.0/24 のネットワークからのTelnet 接続を許可します。

注: IPSecトンネルを経由しない限り、セキュリティレベルが最も低く設定されたインタフェースへの Telnet接続はできません。

ASDM の管理セッションは **http server enable**と **http** コマンドを介して有効になります。

ssh コマンドは、セキュリティ アプライアンスへの SSH 接続が許可される IP アドレスを設定するために用いられます。たとえば:

```
ASA(config)# ssh 192.168.10.0 255.255.255.0 inside
```

上記の設定例はCisco ASA の inside インタフェースに対して IP アドレス192.168.10.0/24 のネットワークからの SSH 接続を許可します。

クライアントレスWebVPN、SSL VPNクライアント、AnyConnectクライアントの接続は **webvpn** コマンドによって有効になります。以下の設定例は、Cisco ASA において WebVPN が有効に設定されています。この場合、Cisco ASA はWebVPN 接続にデフォルトポートとして TCPポート番号443をリッスンします。

```
http server enable
!
webvpn
 enable outside
```

この特定の設定は機器が **outside** インタフェースから来る攻撃に脆弱であることに注意してください。

この脆弱性はCisco Bug IDCSCsm84110 **(** 登録 **ユーザのみ)** で文章化され、Common Vulnerabilities and Exposures (CVE) の識別子として CVE-2008-2055が割り当てられています。

2. Crafted TLS Packet Vulnerability

トランスポート層セキュリティ（ TLS ）は、Secure Socket Layer （ SSL ）プロトコルの代替で、暗号によって 2つのエンド ポイントの間で安全な通信を提供するプロトコルです。

Cisco PIX と ASA セキュリティ アプライアンスは、さまざまなシナリオで通信の機密性を保護するために、TLS を使用します。PIX と ASAは、これら全てのシナリオにおいて TLS プロトコルの取り扱いに関する脆弱性の影響を受け、特に巧妙に細工された TLS パケットを処理するときに装置のリロードが発生する可能性があります。

注:本脆弱性はこのパケットが機器を宛先とする場合にのみ影響します。機器を通過する場合は本脆弱性の影響を受けません。

以下のリストはCisco ASA 及び PIX において TLS を使用するアプリケーションのいくつかが含まれます。

- クライアントレスWebVPN、SSL VPN クライアント、AnyConnect クライアント接続

- ASDM (HTTPS) 管理セッション
- ネットワーク アクセスのためのカットスルー プロキシ
- 暗号化された音声のインスペクションための TLS プロキシ

クライアントレスWebVPN、SSL VPNクライアント、AnyConnectクライアント接続

クライアントレス WebVPN 接続、SSL VPN クライアント接続,、AnyConnect クライアントの接続は **webvpn**コマンドによって有効になります。以下に、Cisco ASA において WebVPN を有効にしている設定例を示します。この場合、Cisco ASA は WebVPN 接続にデフォルトポートとしてTCPのポート番号443を使用します。

```
http server enable
!
webvpn
 enable outside
```

この特定の設定では、機器が **outside** インタフェースから来る攻撃に脆弱であることに注意してください。

ASDM (HTTPS) 管理セッション

ASDMの管理セッションは **http server enable** と **http** コマンドにより有効になります。以下にリモート HTTPS 管理がASAに設定された例を示します。

```
http server enable
http 192.168.0.0 255.255.255.0 inside
```

この特定の設定は機器が **inside** インタフェースから来る攻撃に脆弱であることに注意してください

ネットワークアクセスのためのカットスループロキシ

カットスループロキシ機能はネットワーク アクセスの前にユーザを認証するために用いられます。以下は、ネットワーク アクセスを許可する前にユーザに認証を要求する設定例です。

```
access-list auth-proxy extended permit tcp any any eq www
access-list auth-proxy extended permit tcp any any eq telnet
access-list auth-proxy extended permit tcp any any eq https
!
aaa authentication match auth-proxy inside LOCAL
aaa authentication secure-http-client
aaa authentication listener https inside port https
```

この脆弱性によって影響を受ける設定には **aaa authentication secure-http-client** または **aaa authentication listener https inside port <port number>** コマンドが含まれます。上記の設定例では機器が inside インタフェースから来る攻撃に脆弱であることに注意してください。

暗号化された音声のインスペクションのための TLS プロキシ

暗号化された音声のインスペクションのための TLS プロキシ機能はセキュリティアプライアンスが復号化、検査および修正（必要に応じて、例えばNAT fixupの実行）することを可能にし、また、SCCP と Session Initiation Protocol (SIP) プロトコルのための VoIP 検査機能の全てが保持される間、音声のシグナリング トラフィックを再び暗号化することを可能にします。いったん音声のシグナリングが復号化されると、プレーンテキスト形式のシグナリングメッセージはインスペクション エンジンに渡されます。セキュリティアプライアンスは IP-Phone と Cisco Unified CallManager、Cisco Unified Communications Manager の間の TLS プロキシとして振舞うことによりこれを実現します。これらの機器とセキュリティアプライアンスの間には TLSセッションが張られ、TCP ポート 2443 と 5061 が使用されます。

Cisco PIX及びASA セキュリティ アプライアンスにおいて暗号化された音声のインスペクションをサポートしている設定がおこなわれているかを確認するには、機器に口グインして **show service-policy | include tls** CLIコマンドを発行します。もし出力にテキスト **tls-proxy: active** といくつかの統計情報が含まれていれば、その機器には脆弱性のある設定がされています。以下に Cisco ASA セキュリティ アプライアンスに脆弱性のある例を示します。

```
ASA# show service-policy | include tls
      Inspect: sip tls-proxy myproxy, packet 0, drop 0, reset-drop 0
               tls-proxy: active sess 0, most sess 0, byte 0
      Inspect: skinny tls-proxy myproxy, packet 0, drop 0, reset-drop 0
               tls-proxy: active sess 0, most sess 0, byte 0
ASA#
```

この脆弱性は Cisco Bug ID CSCsm26841 (登録ユーザのみ) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-2056.

3. Instant Messenger Inspection Vulnerability

Cisco ASA と PIX のインスタントメッセンジャー（IM） のインスペクション エンジンは、お客様のネットワークにおける IMアプリケーション使用のきめの細かいコントロールの適用に用いられます。インスタント メッセージングの検査が有効になっている場合、Cisco ASAとCisco PIXはサービス妨害の脆弱性による影響を受けます。

IM インスペクション機能とその設定の詳細については、以下で確認可能です。

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/inspect.html#wp1479354

この脆弱性は Cisco Bug ID CSCso22981 (登録ユーザのみ) で文章化され、Common Vulnerabilities and Exposures (CVE) の識別子として CVE-2008-2055が割り当てられています。

4. Vulnerability Scan Denial of Service

Cisco ASAとPIXセキュリティアプライアンスは、TCPポート443に対して脆弱性をスキャンされたときに、サービス妨害の脆弱性の影響を受けます。特定の脆弱性スキャナーによってシステムがリロードする可能性があります。

注: この脆弱性は機器を宛先とするTCPポート番号443のトラフィックにより影響を受けます。Cisco ASA及びPIXセキュリティ アプライアンスはクライアントレスWebVPN、SSL VPN クライアント、AnyConnectクライント接続する場合、HTTPS 管理セッション, ネットワークアクセスのためのカットスループロキシ, 暗号化された音声のインスペクションのためのTLSプロキシにTCPポート番号443を使用します。詳細は「巧妙に細工されたTLSパケットの脆弱性」のこれらのサービスにおける追加情報を参照ください。

この脆弱性は Cisco Bug ID CSCsj60659 (**登録ユーザのみ)** で文章化され、Common Vulnerabilities and Exposures (CVE) の識別子として CVE-2008-2058 が割り当てられています。

5. Control-plane Access Control List Vulnerability

コントロールプレーン ACL はセキュリティアプライアンスを宛先とするトラフィックから保護されるよう設計されています。Cisco ASA 及び PIX には、コントロールプレーン ACL が初期設定後に動作しない場合があるという脆弱性があります。

以下の例では **show running-config | include control-plane** コマンドを使用してコントロールプレーンACLがその機器に設定されているかを確認することが出来ます。

```
ASA# show running-config | include control-plane
access-group 101 in interface inside control-plane
ASA#
```

この脆弱性は Cisco Bug ID CSCsm67466 (**登録ユーザのみ)**で文章化され、Common Vulnerabilities and Exposures (CVE) の識別子として CVE-2008-2058 が割り当てられています。

脆弱性スコア詳細

Ciscoは Common Vulnerability Scoring System（ CVSS ） のVersion 2.0に基づいた脆弱性のスコアリングを提供しています。

CVSSは、脆弱性、重要度を示唆するもので、優先度、緊急性を決定する手助けとなる標準ベースの評価法です。

Ciscoは基本評価（ Base Score ）および現状評価スコア （ Temporal Score ）を提供いたします。お客様はこれらを用いて環境評価スコア （ Environmental Score ）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

Ciscoは以下の URLにてCVSSに関するFAQを提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html.

またCiscoは個々のネットワークにおける環境影響度を算出するツールを以下のURLにて提供しています。

http://intellishield.cisco.com/security/alertmanager/cvss.

CSCsm84110 - Crafted TCP ACK Packet Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsm26841 - Crafted TLS Packet Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCso22981 - Instant Messenger Inspection Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsj60659 - Vulnerability Scan Denial of Service Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vecto	Access Complexity	Authentication	Confidentiality Impact	Integrity Impa	Availability Impact

r				ct	
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsm67466 - Control-plane Access Control List Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	None	None
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

最初の 4 つの脆弱性の利用に成功した場合、機器のリロードが発生する可能性があります。継続的な攻撃は結果的にサービス妨害(DoS)攻撃になります。 5 つ目の脆弱性の利用に成功した場合、攻撃者にコントロールプレーンアクセスリスト (ACL)をバイパスされ、悪意のあるトラフィックを機器に送られる可能性があります。

ソフトウェアバージョンおよび修正

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。情報が不明確な場合は、Cisco Technical Assistance Center（TAC）もしくは契約している保守会社にお問い合せください。

以下は、個々の脆弱性に関するソフトウエア（最初に修正されたソフトウエア）のリリース一覧です。

Vulnerability	Affected Release	First Fixed Release
Crafted TCP ACK Packet Vulnerability	7.0	Not vulnerable
	7.1	7.1(2)70

	7.2	7.2(4)
	8.0	8.0(3)10
	8.1	Not vulnerable
Crafted TLS Packet Vulnerability	7.0	Not vulnerable
	7.1	Not vulnerable
	7.2	Not vulnerable
	8.0	8.0(3)9
	8.1	8.1(1)1
Instant Messenger Inspection Vulnerability	7.0	Not vulnerable
	7.1	Not vulnerable
	7.2	7.2(4)
	8.0	8.0(3)10
	8.1	8.1(1)2
Vulnerability Scan Denial of Service	7.0	Not vulnerable
	7.1	Not vulnerable
	7.2	7.2(3)2
	8.0	8.0(2)17
	8.1	Not vulnerable
Control-plane Access Control List Vulnerability	7.0	Not vulnerable
	7.1	Not vulnerable
	7.2	Not vulnerable
	8.0	8.0(3)9
	8.1	Not vulnerable

以下のサイトよりPIXに関する修正版ソフトウェアのダウンロードが可能です。

http://www.cisco.com/pcgi-bin/tablebuild.pl/pix?psrtdcat20e2

以下のサイトよりASAに関する修正版ソフトウウェアのダウンロードが可能です。

http://www.cisco.com/pcgi-bin/tablebuild.pl/asa?psrtdcat20e2

回避策

本セキュリティアドバイザリは複数の違った脆弱性について記述しています。これらの脆弱性と個々の回避策は互いに独立しています。

Crafted TCP ACK Packet Vulnerability

回避策およびベストプラクティスとして、お客様ネットワーク内の信頼できるホストからのみのTelnet, SSH および ASDM接続を許可して下さい。

加えて、ネットワークの入り口となる機器での受信トラフィックに対する防御のため、トランジット ACL(tACL) ポリシーの一部として TCP ポート 22 , 23 , 80および 443へのパケットを拒否するフィルタをネットワーク全体にわたって配備することが出来ます。このポリシーはフィルタが適用されるネットワーク機器およびその背後の機器を防御するよう構成される必要があります。TCP ポート 22, 23, 80 および 443 を使うパケットに対するフィルタは、信頼できるクライアントからのトラフィックのみが許可されるよう、脆弱性のあるネットワーク機器の前面に配備される必要があります。

tACLについての追加情報は "Transit Access Control Lists : Filtering at Your Edge" にあります。

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

Crafted TLS Packet Vulnerability

この脆弱性に回避策はありません。

Instant Messenger Inspection Vulnerability

この脆弱性の唯一の回避策はセキュリティ機器の IMインスペクションを無効にすることです。

Vulnerability Scan Denial of Service

この脆弱性に回避策はありません。

Control-plane Access Control List Vulnerability

この脆弱性に回避策はありません。

ネットワーク内のCisco機器に配備できる追加的な緩和技術が本アドバイザリの付随ドキュメント

（Cisco Applied Mitigation Bulletin）にあります。

http://www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a00809a8359.html

修正ソフトウェアの入手

Ciscoは本脆弱性の影響を受けるお客様のために、本脆弱性対処用の無償のソフトウェアを提供しています。ソフトウェアの導入を行う前に、機能のソフトウェアの互換性およびお客様のネットワーク環境に特有の問題に関して確認いただくか、あるいはお客様のメンテナンスプロバイダーにご相談ください。

お客様がインストールしたり、サポートを受けたりできるのは、ご購入いただいたフィーチャーセットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html, にあるCiscoのソフトウェア ライセンスの条項または

http://www.cisco.com/public/sw-center/sw-usingswc.shtml. にある Cisco.com のダウンロードに示されるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、"psirt@cisco.com" もしくは "security-alert@cisco.com" にお問い合わせいただくことはご遠慮ください

ご契約を有するお客様

ご契約を有するお客様は、通常の経路でそれを入手してください。ほとんどのお客様は、Ciscoのワールドワイドウェブサイト上の ソフトウェアセンターから入手することができます。

http://www.cisco.com.

サードパーティのサポート会社をご利用のお客様

Cisco パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からCisco製品の提供または保守を受けている お客様は、該当するサポート会社に連絡し、本脆弱性に関する適切な処置について支持と支援を受けてください。

回避策の効果は、お客様の状況、使用製品、ネットワークトポロジー、トラフィックの性質や組織の目的に依存します。影響製品が多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、お客様のサービスプロバイダーやサポート組織にご相談ください。

サービス契約をご利用でないお客様

Ciscoから直接購入したがCiscoのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Ciscoの Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。TAC の連絡先は次のとおりです。

- +1 800 553 2447 (北米内からのフリー ダイヤル)
- +1 408 526 7209 (北米以外からの有料通話)
- 電子メール: tac@cisco.com

無料アップグレードの対象であることをご証明いただくために、製品のシリアル番号を用意し、このお知らせのURLを知らせてください。サポート契約をご利用でないお客様に対する無料アップグレードは、TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、http://www.cisco.com/warp/public/687/Directory/DirTAC.shtmlを参照してください。

不正利用事例と公表

Cisco PSIRTにおいて、現在本アドバイサリ内で記載されている脆弱性を悪用する事例や不正利用は確認されておりません。

この脆弱性はCisco社内の試験とサービスリクエストのトラブルシューティング過程において発見されました。

この通知のステータス: FINAL

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を示唆するものでもありません。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Cisco Systemsは本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して、独自の複製･ 意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリーは、以下のCiscoのワールドワイドウェブサイト上に掲載されます。

http://www.cisco.com/en/US/products/products_security_advisory09186a00809a8354.shtml

ワールドワイドのウェブ以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版がCisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

この通知に関する今後の最新情報は、いかなるものもCiscoのワールドワイドウェブに掲載される

予定です。しかしながら、前述のメーリングリストもしくはニュースグループに対し積極的に配信されるとは限りません。この問題に関心があるお客様は上記 URLにて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2008-June-04	Initial public release

シスコセキュリティ手順

Cisco製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびCiscoからセキュリティ情報を入手するための登録方法について詳しく知るには、Ciscoワールドワイドウェブサイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm にアクセスしてください。このページにはCiscoのセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。全てのCiscoセキュリティアドバイザリは http://www.cisco.com/go/psirt で確認することができます。