Cisco ASAソフトウェアの複数の脆弱性

アドバイザリーID : cisco-sa-20131009-asa
初公開日 : 2013-10-09 16:00
最終更新日 : 2013-12-13 05:29
バージョン 2.2 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCui34914 CSCtt36737 CSCud37992 CSCuf52468 CSCug83401 CSCui77398 CSCue18975 CSCuh44815 CSCub98434 CSCua22709 CSCug03975

CVE-2013-5515
CVE-2013-3415
CVE-2013-5513
CVE-2013-5511
CVE-2013-5512
CVE-2013-5542
CVE-2013-5510
CVE-2013-5508
CVE-2013-5509
CVE-2013-5507

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適応型セキュリティアプライアンス(ASA)ソフトウェアは、次の脆弱性の影響を受けます。

- IPsec VPNにおける巧妙に細工されたICMPパケットによるDoS脆弱性
- SQL*Netインスペクションエンジンの DoS脆弱性
- デジタル証明書認証バイパスの脆弱性
- リモートアクセスVPN認証バイパスの脆弱性
- デジタル証明書HTTP認証バイパスの脆弱性
- HTTPディープパケットインスペクションに関するDoS脆弱性
- DNSインスペクションに関するDoS脆弱性
- AnyConnect SSL VPNのメモリ枯渇によるDoS脆弱性
- SSL VPN Webポータルの DoS脆弱性
- 巧妙に細工されたICMPパケットによるDoS脆弱性

これらの脆弱性は互いに独立しています。いずれかの脆弱性の影響を受けるリリースが、他の脆弱性の影響を受けることはありません。

IPsec VPNの巧妙に細工されたICMPパケットのサービス拒否の脆弱性、SQL*Netインスペクションエンジンのサービス拒否の脆弱性、HTTPディープパケットインスペクションのサービス拒否の脆弱性、DNSインスペクションのサービス拒否の脆弱性、およびSSL VPN Web Portalのサービス拒否の脆弱性が不正利用されると、該当デバイスのリロードが発生し、サービス拒否(DoS)状態が発生するするする可能性があります。

デジタル証明書認証バイパスの脆弱性、リモートアクセスVPN認証バイパスの脆弱性、およびデジタル証明書HTTP認証バイパスの脆弱性が悪用されると、認証バイパスが発生し、攻撃者がリモートアクセスVPN経由で内部ネットワークにアクセスしたり、Cisco Adaptive Security Device Management(ASDM)経由で該当システムに管理アクセスしたりする可能性があります。

AnyConnect SSL VPNのメモリ枯渇に関するDoS脆弱性が悪用されると、使用可能なメモリが枯渇し、結果としてシステムが不安定になり、該当システムが応答しなくなり、トラフィックの転送が停止する可能性があります。

巧妙に細工されたICMPパケットによるサービス拒否(DoS)の脆弱性が不正利用されると、該当システムを通過する有効な接続がドロップされるか、システムのリロードが引き起こされ、サービス拒否(DoS)状態が発生する可能性があります。

シスコはこれら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。一部の脆弱性には回避策があります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131009-asa

注： Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用のCisco Firewall Services Module(FWSM)は、SQL*Netインスペクションエンジンのサービス妨害(DoS)の脆弱性の影響を受ける可能性があります。Cisco FWSMに影響する脆弱性に関しては、別途Cisco Security Advisoryが公開されています。このアドバイザリは次のリンクに掲載されています。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131009-fwsm

該当製品

Cisco ASA 5500シリーズ適応型セキュリティアプライアンス、Cisco ASA 5500-X次世代ファイアウォール、Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュール、Cisco ASA 1000Vクラウドファイアウォールの Cisco ASAソフトウェアは、複数の脆弱性の影響を受けます。影響を受けるCisco ASAソフトウェアのバージョンは、

脆弱性によって異なります。影響を受ける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 バージョンおよび修正」セクションを参照してください。

脆弱性のある製品

IPsec VPNにおける巧妙に細工されたICMPパケットによるDoS脆弱性

この脆弱性が存在するには、Cisco ASAソフトウェアに、アクティブなトラフィックがトンネルを通過するIPsec VPNトンネルが少なくとも1つ存在している必要があります。この脆弱性は、問題のパケットがSSL/TLSベースのVPNトンネルを通過する場合には不正利用できません。

Cisco ASAソフトウェアでIPSec VPNを使用するように設定されているかどうかを確認するには、 show running-config crypto mapコマンドを使用して、Cisco ASAの少なくとも1つのインターフェイスにクリプトマップが適用されていることを確認します。次の例は、outside_mapという名前の暗号マップが outsideインターフェイスに適用されているCisco ASAを示しています。

```
ciscoasa# sh running-config crypto map
[...]
crypto map outside_map interface outside
```

注：Cisco ASAソフトウェアには、デフォルトではどのインターフェイスにも適用されるクリプトマップがありません。

SQL*Netインスペクションエンジンの DoS脆弱性

Cisco ASAソフトウェアは、SQL*Netインスペクションが有効な場合、この脆弱性の影響を受けます。

SQL*Netインスペクションが有効になっているかどうかを確認するには、 show service-policy | include sqlnetコマンドを使用して、出力が返ることを確認します。次の例は、SQL*Netインスペクションが有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show  service-policy | include sqlnet
  Inspect: sqlnet, packet 0, drop 0, reset-drop 0
```

注： SQL*Netインスペクションはデフォルトで有効になっています。

デジタル証明書認証バイパスの脆弱性

Cisco ASAソフトウェアは、次のいずれかの場合にこの脆弱性の影響を受けます。

- クライアントレスSSL VPNまたはAnyConnect SSL VPNがデジタル証明書認証を使用するように設定されている
- Cisco ASDMがデジタル証明書認証を使用するように設定されている

クライアントレスSSL VPNまたはAnyConnect SSL VPNがデジタル証明書認証を使用するように設定されているかどうかを確認するには、 show running-config webvpnコマンドを使用します。VPN機能に対してデジタル証明書認証が有効になっているかどうかを確認するには、 show running-config tunnel-group <Tunnel_Group_Name>(<Tunnel_Group_Name>はクライアントレスSSL VPNプロファイルまたはAnyConnect SSL VPNプロファイルに関連付けられたトンネルグループ)を使用し、tunnel-group webvpn-attributesの下にauthentication certificateまたはauthentication aacertificateコマンドがあることを確認します。

次の例は、クライアントレスSSL VPNまたはAnyConnect SSL VPN機能がoutsideインターフェイスで有効になっており、AnyConnect-TGという名前のトンネルグループで証明書認証が有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config webvpn
webvpn
 enable outside

ciscoasa# show running-config tunnel-group AnyConnect-TG
[...]
tunnel-group DefaultRAGroup webvpn-attributes
 authentication aaa certificate
```

Cisco ASDMがデジタル証明書認証を使用するように設定されているかどうかを確認するには、show running-config httpコマンドを使用して、http server enabledコマンドとhttp authentication-certificate <Interface_name>コマンドの両方が存在することを確認します。次の例は、Cisco ASDMと証明書認証が内部インターフェイスで有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config http
http server enable
[...]
http authentication-certificate inside
```

一部のCisco ASAバージョンでは、ssl certificate-authentication interface <Interface_name> port <Port_Number>コマンドが、http authentication-certificate <Interface_name>コマンドの代わりに使用されていました。

注：デジタル証明書認証はデフォルトで無効になっています。この脆弱性は、Cisco ASA 5505、Cisco ASA 5510、Cisco ASA 5520、Cisco ASA 5540、およびCisco ASA 5550製品には影響しません。

リモートアクセスVPN認証バイパスの脆弱性

Cisco ASAソフトウェアは、次のすべての条件に当てはまる場合に、この脆弱性の影響を受けます。

1. クライアントレスVPNまたはAnyConnect VPN、IKEv1およびIKEv2リモートIPsec VPN、L2TP/IPsec VPNのいずれかに設定されている
2. リモートVPNは、LDAPを使用してリモートAAAサーバ経由で認証されます
3. override-account-disableオプションは、tunnel-group general-attributes設定の下で設定されます。

リモートVPNの認証に他のリモートAAAサーバまたはローカルAAAサーバを使用するCisco ASAソフトウェアは、この脆弱性の影響を受けません。また、LAN-to-LAN IPsec VPNが設定されたCisco ASAソフトウェアは、この脆弱性の影響を受けません。

LDAP AAAサーバとoverride-account-disableコマンドがtunnel-group general-attributes設定の下に設定されているかどうかを確認するには、show running-config tunnel-group <Tunnel_Group_Name>コマンドを使用します。

次の例は、AAA-LDAP-SERVERという名前のリモートAAAサーバ経由でトンネルグループAnyConnect-TGを使用し、override-account-disableオプションを有効にして、リモートVPNセッションを認証するように設定されたCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config tunnel-group AnyConnect-TG
tunnel-group test general-attributes
 authentication-server-group AAA-LDAP-SERVER
 override-account-disable
```

また、show aaa-server protocol ldapコマンドを使用して、トンネルグループに関連付けられたリモートAAAサーバがLDAPサーバであることを確認します。次の例は、LDAP上で実行されるAAA-LDAP-SERVERという名前のAAAサーバが設定されたCisco ASAを示しています。

```
ciscoasa# show aaa-server protocol ldap
Server Group:    AAA-LDAP-SERVER
Server Protocol: ldap
[...]
```

注：override-account-disableコマンドはデフォルトで無効になっています。

デジタル証明書HTTP認証バイパスの脆弱性

Cisco ASDMでデジタル証明書クライアント認証が有効になっている場合、Cisco ASAソフトウェアはこの脆弱性の影響を受けます。show running-config http コマンドを使用して、authentication-certificate <Interface_Name>コマンドが設定されていることを確認します。次の例は、http authentication-certificateコマンドが内部インターフェイスで有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config http
http server enable
[...]
http authentication-certificate inside
```

一部のCisco ASAバージョンでは、ssl certificate-authentication interface <Interface_name>port <Port_Number>コマンドが、http authentication-certificate <Interface_name>コマンドの代わりに使用されていました。

注：Cisco ASDMでは、デジタル証明書認証はデフォルトで無効になっています。

HTTPディープパケットインスペクションに関するDoS脆弱性

Cisco ASAソフトウェアは、HTTPディープパケットインスペクション(DPI)が次のいずれかのオプションで設定されている場合に、この脆弱性の影響を受けます。

- spoof-serverパラメータオプションがイネーブルになっている
- maskオプションが有効で、本文にactive-xが含まれるHTTP応答を検査しています
- maskオプションが有効になっており、本文にjava-appletを含むHTTP応答を検査しています

これらの設定のいずれかが存在するかどうかを確認するには、show running-config policy-map type inspect httpコマンドを使用します。次の例は、HTTP_DPI_PMというHTTP DPIポリシーが設定され、spoof-serverオプションが有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config policy-map type inspect http
!
policy-map type inspect http HTTP_DPI_PM
 parameters
  spoof-server "Apache"
 !
```

注：HTTPインスペクションエンジンとHTTP DPIはデフォルトで無効になっています。この脆弱性は、Cisco ASA 5505、Cisco ASA 5510、Cisco ASA 5520、Cisco ASA 5540、およびCisco ASA 5550製品には影響しません。

DNSインスペクションに関するDoS脆弱性

Cisco ASAソフトウェアは、DNSアプリケーション層プロトコルインスペクション(ALPI)エンジンがTCP経由でDNSパケットを検査するように設定されている場合、この脆弱性の影響を受けます。

DNS ALPIエンジンがTCP経由のDNSパケットを検査しているかどうかを確認するには、show running-config access-list <acl_name>コマンドを使用します。ここで、acl_nameは、DNS検査が適用されるclass-mapで使用されるアクセスリストの名前です。

これは、show running-config class-mapコマンドとshow running-config policy-mapコマンドを使用して確認できます。

次の例は、DNS ALPIエンジンがTCP上のDNSパケットを検査するように設定されているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config access-list
[...]
access-list DNS_INSPECT_ACL extended permit tcp any any
[...]
```

または

```
ciscoasa# show running-config access-list
[...]
access-list DNS_INSPECT_ACL extended permit ip any any
[...]
ciscoasa# show running-config class-map
!
class-map DNS_INSPECT_CP
 match access-list DNS_INSPECT
[...]
ciscoasa# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  [...]
 class DNS_INSPECT_CP
  inspect dns preset_dns_map
!
```

注：Cisco ASAソフトウェアは、デフォルトではTCP経由のDNSパケットを検査しません。

AnyConnect SSL VPNのメモリ枯渇によるDoS脆弱性

AnyConnect SSL VPNが設定されている場合、Cisco ASAソフトウェアに脆弱性が存在します。クライアントレスSSL VPN、IKEv1/IKEv2 IPsecリモートおよびLAN-to-LAN VPN、またはL2TP/IPsec VPN用に設定されたCisco ASAソフトウェアは、この脆弱性の影響を受けません。

Cisco ASAソフトウェアでAnyConnect SSL VPNが設定されているかどうかを確認するには、show running-config webvpnを使用して、svc enble（Cisco ASAソフトウェアバージョン8.4以降）またはanyconnect enable（Cisco ASAソフトウェアバージョン8.4以降）コマンドが存在することを確認します。

次の例は、AnyConnect SSL VPN機能が有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config webvpn
webvpn
 [...]
 svc enable
```

注：AnyConnect SSL VPNはデフォルトで無効になっています。

SSL VPN WebポータルのDoS脆弱性

クライアントレスSSL VPNまたはAnyConnect SSL VPNが設定されている場合、Cisco ASAソフトウェアに脆弱性が存在します。IKEv1/IKEv2 IPsecリモートおよびLAN-to-LAN VPN、またはL2TP/IPsec VPN用に設定されたCisco ASAソフトウェアは、この脆弱性の影響を受けません。

SSL VPNが有効になっているかどうかを確認するには、show running-config webvpnコマンドを使用します。

次の例は、outsideインターフェイスでSSL VPN機能が有効になっているCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config webvpn
     webvpn
     enable outside
```

注：SSL VPNはデフォルトで無効になっています。

巧妙に細工されたICMPパケットによるDoS脆弱性

ICMPインスペクションエンジンがファイアウォールを通過するICMPパケットを検査するように設定されている場合、またはファイアウォールインターフェイスを対象とするICMPパケットの処理が許可されている場合、Cisco ASAソフトウェアには脆弱性が存在します

Cisco ASAソフトウェアのデフォルトの動作では、ファイアウォールインターフェイスへのすべてのICMPトラフィックが許可および処理されます。つまり、デフォルトのCisco ASAソフト

ウェア設定には脆弱性が存在します。デフォルトのICMPポリシーはファイアウォール設定には表示されませんが、インターフェイスでIPバージョン6が有効になっている場合は、コマンドicmp deny any <interface_name>およびipv6 icmp deny any <interface_name>を使用することで、このデフォルトのICMPポリシーを無効にできます。これら2つのコマンドのいずれかが設定されている場合、設定に表示されます。デフォルトのICMPポリシーが無効になっているかどうかを確認するには、show running-config icmp | include deny anyコマンドを使用して、ファイアウォールで設定された各インターフェイスの出力が返されることを確認します。
IPv6が有効なインターフェイスがある場合、ICMPv6のデフォルトのICMPポリシーが無効になっていることを確認するには、show running-config ipv6 | include icmp deny anyコマンドを使用して、ファイアウォールに設定されたIPv6対応インターフェイスごとに出力が返されることを確認します。コマンドから空の出力が返された場合、または出力にファイアウォールインターフェイスのサブセットに設定が適用されていることが示された場合、管理者はシステムが脆弱であると考える必要があります。

ファイアウォール宛ての特定のICMPパケットを許可するような方法で、デフォルト以外のICMPインターフェイスポリシーがデバイスに設定されているかどうかを確認するには、show running-config icmp | include permitおよびshow running-config ipv6 | include icmp permitコマンドを使用して、ファイアウォールに設定された各インターフェイスについて返される出力を確認します。
ICMPパケットを許可する設定がファイアウォールインターフェイスのサブセットに適用されていることがコマンドによって示されている場合、管理者はシステムが脆弱であると考える必要があります。

次の例は、ASAファイアウォールのOutsideインターフェイス宛てのICMPエコー応答パケットを許可するように設定された非デフォルトのICMPポリシーがCisco ASAソフトウェアに設定されていることを示しています。

```
ciscoasa#show running-config icmp | include permit
icmp permit any echo-reply outside
icmp permit any echo-reply dmz1
icmp permit any unreachable outside
icmp permit any echo outside
```

```
ciscoasa#show running-config ipv6 | include permit icmp
ipv6 icmp permit any echo outside
ipv6 icmp permit any echo-reply outside
ipv6 icmp permit any neighbor-advertisement outside
```

ICMP検査エンジンがファイアウォールを通過するICMPパケットを検査するように設定されているかどうかを確認するには、show running-config | include inspect icmp コマンドを使用して

、inspect icmp コマンドが存在することを確認します。inspect icmp errorのみが設定されている設定には脆弱性はありません。

次の例は、ASAファイアウォールを通過するICMPパケットを検査するようにICMPインスペクションエンジンが設定されたCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config | include inspect icmp
inspect icmp
```

注：ICMPインスペクションエンジンは、デフォルトでは有効になっていません。

実行中のソフトウェアバージョンの確認

脆弱性のあるバージョンの Cisco ASA ソフトウェアがアプライアンスで実行されているかどうかを知るには、show version コマンドを発行します。次の例は、Cisco ASAソフトウェアバージョン8.4(1)を実行しているデバイスを示しています。

```
ciscoasa#show version | include Version
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
```

Cisco ASDMを使用してデバイスを管理している場合は、ログインウィンドウまたはCisco ASDMウィンドウの左上隅に表示される表でソフトウェアバージョンを確認できます。

脆弱性を含んでいないことが確認された製品

Cisco ASA-CX Context-Aware Securityは、これらの脆弱性には該当しません。

Cisco FWSMを除き、これらの脆弱性の影響を受けるシスコ製品は現在確認されていません。

詳細

Cisco適応型セキュリティアプライアンス(ASA)ソフトウェアは、Cisco ASA 5500シリーズ適応型セキュリティアプライアンス、Cisco ASA 5500-X Next Generation Firewall、Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュール(ASASM)、Cisco ASA 1000Vクラウドファイアウォールで使用されるオペレーティングシステムです。Cisco ASAファミリは、ファイアウォール、侵入防御システム(IPS)、Anti-X、VPNなどのネットワークセキュリティサービスを提供します。

IPsec VPNにおける巧妙に細工されたICMPパケットによるDoS脆弱性

IPSecコードの脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを

引き起こす可能性があります。

この脆弱性は、アクティブなVPNトンネルを通過するパケットを復号化するコードのエラーに起因します。特に、復号化操作後に巧妙に細工されたICMPパケットをコードが適切に処理できていません。攻撃者は、アクティブなVPNトンネルを介して巧妙に細工されたICMPパケットを送信することにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は復号化操作を実行するデバイスのリロードを引き起こす可能性があります。

注：この脆弱性は、アクティブなIPsec VPNトンネルを通過するICMPトラフィックによってのみ引き起こされます。この脆弱性は、シングルおよびマルチコンテキストモードの両方でルーテッドモードに設定されたCisco ASAソフトウェアに影響を与えます。この脆弱性は、ICMPおよびICMPv6パケットによって引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCue18975(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposure(CVE)IDとしてCVE-2013-5507が割り当てられています。

SQL*Netインスペクションエンジンの DoS脆弱性

SQL*Netインスペクションエンジンコードの脆弱性により、認証されていないリモートの攻撃者が該当システムのリロードを引き起こす可能性があります。

この脆弱性は、セグメント化されたTransparent Network Substrate(TNS)パケットの不適切な処理に起因します。攻撃者は、該当システムを介して、巧妙に細工された一連のセグメント化TNSパケットを送信することにより、この脆弱性を不正利用する可能性があります。

注：この脆弱性は、Cisco ASA SQL*Netインスペクションエンジンによって検査された通過トラフィックによってのみ、不正利用が可能です。この脆弱性は、シングルおよびマルチコンテキストモードの両方で、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの両方に影響します。この脆弱性は、IPバージョン4(IPv4)およびIPバージョン6(IPv6)トラフィックによって引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCub98434(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5508が割り当てられています。

デジタル証明書認証バイパスの脆弱性

Cisco ASAソフトウェアのSSL証明書検証コードの脆弱性により、認証されていないリモートの攻撃者が証明書認証をバイパスできる可能性があります。

この脆弱性は、認証フェーズでクライアントが巧妙に細工した証明書を処理する際のエラーに起因します。攻撃者は、巧妙に細工された証明書を使用して該当システムへの認証を試みることにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は証明書認証

をバイパスできる可能性があります。Cisco ASAの設定によっては、これにより攻撃者がクライアントレスSSL VPNまたはAnyconnect SSL VPN経由でネットワークの認証とアクセスを行ったり、Cisco Adaptive Security Device Management(ASDM)経由で管理管理アクセスを取得したりできる場合があります。

この脆弱性は、クライアントレスSSL VPNおよびAnyConnect SSL VPN用のクライアントデジタル証明書認証、またはCisco ASDM経由のリモート管理用に設定されたCisco ASAソフトウェアに影響を与えます。

Cisco ASA 5505、Cisco ASA 5510、Cisco ASA 5520、Cisco ASA 5540、およびCisco ASA 5550で稼働するCisco ASAソフトウェアは、この脆弱性の影響を受けません。

注：この脆弱性の不正利用に使用できるのは、該当デバイス宛てのトラフィックのみです。この脆弱性は、シングルおよびマルチコンテキストモードにおいて、ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードに設定されたCisco ASAソフトウェアに影響を与えます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。

この脆弱性は、Cisco Bug ID CSCuf52468(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5509が割り当てられています。

リモートアクセスVPN認証バイパスの脆弱性

Cisco ASAソフトウェアのリモートアクセスVPN機能の認証コードにおける脆弱性により、認証されていないリモートの攻撃者がリモートVPN認証をバイパスし、内部ネットワークへのリモートアクセスを可能にする可能性があります。

この脆弱性は、トンネルグループのgeneral-attributesで override-account-disableオプションが設定されている場合に、リモートAAA LDAPサーバから受信されるLDAP応答パケットの解析が不適切であることに起因します。攻撃者は、リモートVPN経由で該当システムへの認証を試みることにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は認証をバイパスし、リモートVPN経由でネットワークにアクセスできる可能性があります。

この脆弱性は、クライアントレスまたはAnyConnect SSL VPN、IKEv1およびIKEv2リモートIPsec VPN、およびL2TP/IPsec VPNが設定されたCisco ASAソフトウェアに影響を与えます。さらに、外部AAA LDAPサーバをリモートVPN認証サービスに使用する必要があります。リモートAAAサービスに他のプロトコルを使用しているCisco ASAソフトウェア、またはリモートVPNの認証にローカルAAAサーバを使用しているCisco ASAソフトウェアは、この脆弱性の影響を受けません。LAN-to-LAN VPNが設定されているCisco ASAソフトウェアは、この脆弱性の影響を受けません。

IKEv1リモートIPsec VPNおよびL2TP/IPsec VPNで設定されたCisco ASAソフトウェアの場合、攻撃者がこの脆弱性を不正利用するには、トンネルグループのパスワードを知っているか、有効なデジタル証明書を保持している必要があります。いずれの場合も、攻撃者がこの脆弱性を不正利用するには、有効なユーザ名を知っている必要があります。

注：本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。この脆弱性は、シングルコンテキストモードのルーテッドファイアウォールモードでのみ設定されたCisco ASAソフトウェアに影響を与えます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID CSCug83401(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5510が割り当てられています。

デジタル証明書HTTP認証バイパスの脆弱性

Cisco Adaptive Security Device Management(ASDM)を介したリモート管理の認証コードにおける脆弱性により、認証されていないリモートの攻撃者がデジタル証明書認証をバイパスできる可能性があります。設定によっては、攻撃者がCisco ASDM経由で管理インターフェイスに管理者としてリモート接続し、影響を受けるシステムを完全に制御できる可能性があります。

この脆弱性は、クライアント側のデジタル証明書認証を有効にする authentication-certificateオプションの実装エラーに起因します。攻撃者は、Cisco ASDMが有効になっている該当システムのインターフェイスへの認証を試みることにより、この脆弱性を不正利用する可能性があります。

注：本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。この脆弱性は、シングルおよびマルチコンテキストモードにおいて、ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードに設定されたCisco ASAソフトウェアに影響を与えます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。この脆弱性を不正利用するには、TCP 3ウェイハンドシェイクが必要です。

この脆弱性は、Cisco Bug ID CSCuh44815(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5511が割り当てられています。

HTTPディープパケットインスペクションに関するDoS脆弱性

HTTPディープパケットインスペクション(DPI)コードの脆弱性により、認証されていないリモートの攻撃者が該当システムのリロードを引き起こす可能性があります。

この脆弱性は、HTTP DPIエンジンがHTTPパケットを検査しており、 spoof-serverパラメータオプションが有効になっているか、応答本文にactive-xまたはjava-appletを含むHTTP応答を検査し

てマスクするようにCisco ASAソフトウェアが設定されている場合に、競合状態が適切に処理されないことに起因します。攻撃者は、該当システムを介して巧妙に細工されたHTTP応答を送信することにより、この脆弱性を不正利用する可能性があります。

注：この脆弱性は、HTTP DPIエンジンによって検査された通過トラフィックによってのみ不正利用が可能です。この脆弱性は、シングルおよびマルチコンテキストモードにおいて、ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードに設定されたCisco ASAソフトウェアに影響を与えます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID CSCud37992(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5512が割り当てられています。

DNSインスペクションに関するDoS脆弱性

Cisco ASAソフトウェアのDNSアプリケーション層プロトコルインスペクション(ALPI)エンジンにおける脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、DNSインスペクションエンジンによるサポートされていないDNS over TCPパケットの不適切な処理に起因します。攻撃者は、該当デバイスを介して巧妙に細工されたDNSメッセージをTCP経由で送信することにより、この脆弱性を不正利用する可能性があります。

注：この脆弱性は、DNS ALPIエンジンによって検査された通過トラフィックによってのみ引き起こされます。シングルおよびマルチコンテキストモードの両方において、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの両方で設定されているCisco ASAソフトウェアが、この脆弱性の影響を受けます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID CSCug03975(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5513が割り当てられています。

AnyConnect SSL VPNのメモリ枯渇によるDoS脆弱性

Cisco ASAソフトウェアによるAnyConnect SSL VPNクライアント接続の処理方法における脆弱性により、認証されていないリモートの攻撃者が使用可能なメモリを枯渇させ、該当システムが応答しなくなり、中継トラフィックがドロップされる可能性があります。

この脆弱性は、AnyConnect SSL VPNクライアントの接続解除後に未使用のメモリブロックが適切にクリアされないことに起因します。攻撃者は、切断されたクライアントのIPアドレスにトラフィックを送信することで、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、AnyConnect SSL VPN用に設定されたCisco ASAソフトウェアに影響を与えます。クライアントレスSSL VPN、IKEv1およびIKEv2リモートIPsec VPN、LAN-to-LAN VPN、またはL2TP/IPSEC VPN用に設定されたCisco ASAソフトウェアは、この脆弱性の影響を受けません。

注：この脆弱性は通過トラフィックによってのみ引き起こされます。この脆弱性は、ルーテッドファイアウォールモードおよびシングルコンテキストモードで設定されたCisco ASAソフトウェアにのみ影響します。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID CSCtt36737(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-3415が割り当てられています。

SSL VPN WebポータルのDoS脆弱性

SSL VPNのWebポータルの脆弱性により、認証されていないリモートの攻撃者が該当システムのリロードを引き起こす可能性があります。

この脆弱性は、SSL VPN用に設定されたCisco ASAソフトウェアに対する巧妙に細工されたHTTPS要求の不適切な処理に起因します。攻撃者は、SSL VPNのWebポータルページをターゲットにして巧妙に細工されたHTTPS要求を送信することで、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、クライアントレスSSL VPNまたはAnyConnect SSL VPN用に設定されたCisco ASAソフトウェアに影響を与えます。IKEv1およびIKEv2リモートIPsec VPN、LAN-to-LAN VPN、L2TP/IPSEC VPN用に設定されたCisco ASAソフトウェアは、この脆弱性の影響を受けません。

注：この脆弱性は、該当システム宛てのトラフィックによってのみ引き起こされます。この脆弱性は、ルーテッドファイアウォールモードおよびシングルコンテキストモードで設定されたCisco ASAソフトウェアにのみ影響します。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID CSCua22709(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-5515が割り当てられています。

巧妙に細工されたICMPパケットによるDoS脆弱性

Cisco ASAソフトウェアのICMPパケット処理機能の脆弱性により、認証されていないリモートの

攻撃者が該当デバイスの任意の接続をクリアしてリロードを引き起こし、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、巧妙に細工されたICMPパケットの不適切な処理に起因します。攻撃者は、巧妙に細工された多数のICMPパケットを該当デバイスに送信したり、該当デバイスを通過させることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はファイアウォール上の任意の接続をクリアしたり、該当デバイスのリロードを引き起こしたりして、サービス拒否(DoS)状態を引き起こす可能性があります。

注：この脆弱性は、通過トラフィックおよび該当システム宛てのトラフィックによってトリガーされる可能性があります。この脆弱性は、シングルコンテキストモードまたはマルチコンテキストモードにおいて、ルーテッドファイアウォールモードおよびトランスペアレントファイアウォールモードに設定されたCisco ASAソフトウェアに影響を与えます。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID CSCui77398(登録ユーザ専用)として文書化され、CVE ID CVE-2013-5542が割り当てられています。

回避策

IPsec VPNにおける巧妙に細工されたICMPパケットによるDoS脆弱性

LAN-to-LANトンネルを含むVPN設定では、vpn-filerアクセスリストを実装することで、問題のICMPパケットの復号化を回避できます。次のコマンドは、着信方向と発信方向の両方でDfltGrpPolicyグループポリシーを使用するVPNトンネルを流れるICMPパケットをブロックするアクセスリストを実装します。

```
ciscoasa(config)# access-list DENY_ICMP_ACL deny icmp any any
ciscoasa(config)# access-list DENY_ICMP_ACL permit ip any any
ciscoasa(config)# group-policy DfltGrpPolicy attributes
ciscoasa(config-group-policy)# vpn-filter value DENY_ICMP_ACL
```

注：この脆弱性は復号化処理中に発生するため、この回避策はVPNトンネルを終端する両方のデバイスに実装する必要があります。この回避策は、トンネルの片側だけに適用すると無効になります。

CiscoリモートIPsec VPNについては、この脆弱性を軽減する回避策はありません。

SQL*Netインスペクションエンジンの DoS脆弱性

Cisco ASA SQL*Netインスペクションを無効にすることで、この脆弱性を軽減できます。次のコマンドを使用すると、デフォルトで設定されているSQL*Netインスペクションが無効になります。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect sqlnet
```

デジタル証明書認証バイパスの脆弱性

影響を受ける機能の認証スキーマを変更する以外に、この脆弱性を軽減する回避策はありません。

リモートアクセスVPN認証バイパスの脆弱性

override-account-disableオプションを無効にする以外に回避策はありません。

デジタル証明書HTTP認証バイパスの脆弱性

影響を受ける機能の認証スキーマを変更する以外に、この脆弱性を軽減する回避策はありません。

HTTPディープパケットインスペクションに関するDoS脆弱性

影響を受けるオプションをHTTP DPI設定から削除する以外に回避策はありません

DNSインスペクションに関するDoS脆弱性

管理者は、UDPトラフィックのみが検査のためにDNS ALPIエンジンに送信されるようにすることで、この問題を回避できます。

そのためには、まずUDPトラフィックのみに一致するアクセスリストを作成し、次にそのアクセスリストに一致するクラスマップを作成します。デフォルトでは、Cisco ASAソフトウェアはUDPトラフィック上のDNSのみを検査することに注意してください。次の例は、DNS ALPIエンジンにUDPポート53トラフィックのみを転送するCisco ASAソフトウェアを示しています。

```
ciscoasa# show running-config access-list
access-list DNS_INSPECT extended permit udp any any eq 53

ciscoasa# show running-config class-map
!
class-map DNS_INSPECT_CP
 match access-list DNS_INSPECT
[...]

ciscoasa# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
```

```
 class inspection_default
  inspect ftp
  inspect h323 h225
  [...]
  class DNS_INSPECT_CP
  inspect dns preset_dns_map
!
```

注：TCP経由のDNSトラフィックの検査は、現在Cisco ASAソフトウェアではサポートされていません。この回避策を実装しても、機能が損なわれることはありません。

AnyConnect SSL VPNのメモリ枯渇によるDoS脆弱性

AnyConnect SSL VPN機能を無効にする以外に、回避策はありません。

SSL VPN WebポータルのDoS脆弱性

SSL VPN機能を無効にする以外に、回避策はありません。

巧妙に細工されたICMPパケットによるDoS脆弱性

管理者は、デフォルトのICMPポリシーとICMPインスペクションエンジンを無効にすることで、この脆弱性を回避できます。
デフォルトのICMPポリシーを無効にするには、Cisco ASAソフトウェアの設定されたすべてのインターフェイスに対して icmp deny any <interface_name>コマンドを使用します。ICMPv6のデフォルトのICMPポリシーを無効にするには、Cisco ASAソフトウェアのすべてのIPv6対応インターフェイスに対して ipv6 icmp deny any <interface_name>コマンドを使用します。次の例は、outsideインターフェイスでICMPv6のデフォルトICMPポリシーとデフォルトICMPポリシーを無効にする方法を示しています

```
ciscoasa(config)# icmp deny any outside
ciscoasa(config)# ipv6 icmp deny any outside
```

注：ファイアウォールインターフェイスでICMP処理を無効にすると、管理者がICMP経由でファイアウォールからこれ以上の情報（pingやtracerouteなど）を受信できなくなる可能性があります。 ファイアウォールインターフェイスでICMPv6処理を無効にすると、ネイバー探索パケットとネイバーアドバタイズメントICMPv6パケットが失われるため、ファイアウォールがそのインターフェイスで通信できなくなる場合があります。

ICMPインスペクションエンジンを無効にするには、サービスポリシーに適用されるポリシーマップ内で no inspect icmpコマンドを使用します。
次の例は、 global_policyという名前のポリシーマップでICMPインスペクションエンジンを無効にする方法を示しています。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect icmp
```

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場合は、 http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性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デバイス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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

次のCisco ASAソフトウェアの表の各行には、このアドバイザリに記載された各脆弱性に対する最初の修正リリースが記載されています。表の最後の行には、Cisco ASAメジャーリリースごとに、このアドバイザリに記載されているすべての脆弱性に対する修正を含むリリースバージョンに関する情報が記載されています。これらのリリースバージョン以降のリリースにアップグレードする必要があります。

	7.0	7.1	7.2	8.0	8.1	8.2	8.3	8.4	
IPsec VPNの巧妙に細工されたICMPパケットによるDoS脆弱性 – CSCue18975	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affe
SQL*Netインスペクションエンジンの DoS脆弱性 – CSCub98434	7.2.x以降に移行	7.2.x以降に移行	7.2（5.12）	8.2.x以降に移行	8.2.x以降に移行	8.2（5.44）	8.3（2.39）	8.4(6)	8.5
デジタル証明書認証バイパスの脆弱性 –	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affe

CSCuf52468									
リモートアクセスVPN認証バイパスの脆弱性 – CSCug83401	7.2.x以降に移行	7.2.x以降に移行	7.2（5.12）	8.2.x以降に移行	8.2.x以降に移行	8.2（5.46）	8.3（2.39）	8.4（6.6）	Not affe
デジタル証明書のHTTP認証バイパスの脆弱性 – CSCuh44815	Not affected	Not affected	Not affected	Not affected	Not affected	8.2（5.46）	8.3（2.39）	8.4（6.6）	8.5
HTTPディープパケットインスペクションに関するDoS脆弱性 – CSCud37992	Not affected	Not affected	Not affected	Not affected	Not affected	8.2(5.46)[1]	8.3(2.39)[1]	8.4(5.5)[1]	8.5(
DNSインスペクションに関するDoS脆弱性 – CSCug03975	Not affected	Not affected	Not affected	Not affected	Not affected	8.2（5.46）	8.3（2.39）	8.4(7)	8.5
AnyConnect SSL VPNのメモリ枯渇に関するDoS脆弱性 – CSCtt36737	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	8.4(3)	Not affe
SSL VPN WebポータルのDoS脆弱	Not affected	Not affected	Not affected	8.2.x以降に移行	8.2.x以降に移行	8.2（5.44）	8.3（2.39）	8.4（5.7）	Not affe

性 – CSCua22709									
巧妙に細工されたICMPパケットによるDoS脆弱性 – CSCui77398	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	8.4(7.2)[2]	Not affe
このセキュリティアドバイザリに記載されているすべての脆弱性を修正する推奨リリース	7.2.x以降に移行	7.2.x以降に移行	7.2（5.12）	8.2.x以降に移行	8.2.x以降に移行	8.2(5.46) 以降	8.3(2.39) 以降	8.4(7.2)[2]以降	8.5(降

[1]この脆弱性は、Cisco ASA 5505、Cisco ASA 5510、Cisco ASA 5520、Cisco ASA 5540、およびCisco ASA 5550には影響しません。
[2] 8.7および8.4の修正済みソフトウェアリリースは、2013年10月30日までに入手可能になる予定です。リリースの正確なバージョン番号は現在不明ですが、すべてのCisco ASAソフトウェアバージョン8.7(1.8)以降および8.4(7.2)以降には、このアドバイザリで参照されるすべての脆弱性に対する修正が含まれます。このドキュメントは、最終的なバージョン番号が入手可能になった時点で更新されます。

ソフトウェアのダウンロード

Cisco ASAソフトウェアは、Cisco.comのSoftware Centerからダウンロードできます。
http://www.cisco.com/cisco/software/navigator.html

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 ASA 5500-X Next Generation Firewallについては、 製品>セキュリティ>ファイアウォール>適応型セキュリティアプライアンス(ASA) > Cisco ASA 5500シリーズ適応型セキュリティアプライアンス> <Cisco ASAモデル> >適応型セキュリティアプライアンス(ASA)ソフトウェアに移動します。これらのバージョンの一部は暫定バージョンであり、ダウンロードページの Interimタブを展開すると表示されます。

Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュールの場合は、 製品>シスコインターフェイスとモジュール> Ciscoサービスモジュール> Cisco Catalyst 6500シリーズ/7600シリーズASAサービスモジュール> Adaptive Security Appliance (ASA) Softwareの順に移動します。これらのバージョンの一部は暫定バージョンであり

、ダウンロードページの Interimタブを展開すると表示されます。

Cisco ASA 1000Vクラウドファイアウォールについては、 製品>セキュリティ>ファイアウォール>適応型セキュリティアプライアンス(ASA) > Cisco ASA 1000Vクラウドファイアウォール>適応型セキュリティアプライアンス(ASA)ソフトウェアに移動します。

推奨事項

$propertyAndFields.get("recommendations")

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とその公表は確認しておりません。

このセキュリティアドバイザリに記載されている脆弱性はすべて、カスタマーサポートケースの解決中に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131009-asa

改訂履歴

リビジョン 2.2	2013-December-13	SSL VPN Webポータルの DoS脆弱性に関する情報の一部を修正 – CSCua22709
Revision 2.1	2013年10月18日	CSCui77398に関する追加情報を追加
Revision 2.0	2013年10月17日	「巧妙に細工されたICMPパケットによるDoS脆弱性」(CSCui77398)に関する情報を追加
リビジョン 1.1	2013年10月10日	脆弱性の影響を受けない製品のリストを更新。
リビジョン 1.0	2013年10月9日	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。