Cisco Secure Desktop Cache Cleaner Command Execution Vulnerability

Advisory ID: cisco-sa-20150415-csd

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150415-csd

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。

Revision 1.0

For Public Release 2015 April 15 16:00 UTC (GMT)

目次

要約
該当製品
詳細
脆弱性スコア詳細
影響
ソフトウェア バージョン及び修正
回避策
修正済みソフトウェアの入手
不正利用事例と公式発表
この通知のステータス : Draft
情報配信
更新履歴
シスコ セキュリティ手順

要約

Cisco Secure Desktop のシスコ署名付き Java Archive (JAR) 実行可能ファイル Cache Cleaner コンポーネントの脆弱性は、感染した *.jar* ファイルが実行されるクライアント ホスト上での認証されていないリモート攻撃者による任意のコマンドの実行を可能にします。ユーザの特権を使用してコマンド実行が行われる可能性があります。

Cache Cleaner 機能は 2012 年 11 月から使用が停止されています。

この脆弱性が修正されたソフトウェアは存在しません。感染した *.jar* ファイルを含む Cisco Secure Desktop パッケージはすでに削除されており、ダウンロードできません。

既存の Cisco Secure Desktop パッケージはすべてシスコの管理下にないため、不正利用の可能性を排除するには、お客様自身が Java ブラックリスト制御が最新になっていることを確認することをお勧めします。この脆弱性の対策に関するその他の情報については、このアドバイザリの「回避策」の項を参照してください。

Cisco Secure Desktop をご使用のお客様は、Cisco Host Scan スタンドアロン パッケージに移行する必要があります。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150415-csd

該当製品

脆弱性が存在する製品

Cisco Secure Desktop は、Cisco ASA ソフトウェアと Cisco IOS ソフトウェア SSL VPN サービスに使用できます。

Cisco ASA ソフトウェアの Cisco Secure Desktop 機能が有効に設定されているかどうかを確認するには、 **show webvpn csd** コマンドを使用して、 *Secure Desktop* がインストールされ、有効になっていることを確認します。次の例は、Cisco Secure Desktop バージョン 3.6.6249 が有効になっている Cisco ASA デバイスを示しています。

```
ciscoasa# show webvpn csd
Secure Desktop version 3.6.6249.0 is currently installed and enabled.
```

Cisco IOS ソフトウェアの Cisco Secure Desktop 機能が有効に設定されているかどうかを確認するには、 **show webvpn install status csd** コマンドを使用して、 *Secure Desktop* がインストールされていることを確認します。次の例は、Cisco Secure Desktop バージョン 3.1.0.9 が有効になっている Cisco IOS デバイスを示しています。

```
router#show webvpn install status csd
SSLVPN Package Cisco-Secure-Desktop version installed:
CISCO CSD CAT6K
3,1,0,9
```

この脆弱性は、悪意のある *.jar* ファイルを実行するホストに影響します。Cisco ASA ソフトウェアと Cisco IOS ソフトウェアは、この脆弱性の影響を受けません。

攻撃者はシスコによって署名された *.jar* ファイル内の脆弱性を利用できるため、この脆弱性は Cisco Secure Desktop の使用者だけでなく、任意のユーザに対して利用される可能性があります。

シスコは、感染したバージョンの *.jar* ファイル用の SHA-1 ハッシュを提供しています。このハッシュを使用すれば、Java Blacklist Jar 機能を介した不正利用を阻止できます。また、シスコでは、デフォルトで感染した *. jar* ファイルをブラックリストに追加するように Java に対して要請しています。この変更は Java SE 8 Update 45 で入手できます。その他の詳細については、このアドバイザリの「回避策」の項を参照してください。

脆弱性が存在しない製品

Cisco Host Scan スタンドアロンと CiscoAnyConnect Secure Mobility Client には、感染した *.jar* ファイルが含まれていないため、この脆弱性の影響を受けません。

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco Secure Desktop スイートは、追加のセキュリティ サービスを提供することによって、Cisco ASA と Cisco IOS Clientless および AnyConnect SSL VPN 機能を拡張します。Cache Cleaner 機能は、クライアントレス SSL VPN セッションの終了時点でブラウザ キャッシュから情報を消去するために使用されます。

Cisco Secure Desktop の Cache Cleaner コンポーネントに含まれるシスコ署名付き Java Archive（JAR）実行可能ファイルの脆弱性は、感染した *.jar* ファイルが実行されるクライアント ホスト上での認証されていないリモート攻撃者による任意のコマンドの実行を可能にします。感染したファイルを実行するユーザの特権を使用してコマンド実行が行われる可能性があります。

この脆弱性の原因は、 *cache.jar* ファイルの実行中の制御が不十分であることです。攻撃者は、感染した *. jar* ファイルとその他の悪意のある実行可能ファイルを含む巧妙に作られたパッケージを提供可能な悪意のある Web サイトにユーザをリダイレクトすることによって、この脆弱性を利用できます。

注：この脆弱性は、悪意のある *.jar* ファイルを実行するホストに影響します。Cisco ASA ソフトウェアと Cisco IOS ソフトウェアは、この脆弱性の影響を受けません。

攻撃者はシスコによって署名された *.jar* ファイル内の脆弱性を利用できるため、この脆弱性は Cisco Secure Desktop の使用者だけでなく、任意のユーザに対して利用される可能性があります。

シスコは、感染したバージョンの *.jar* ファイル用の SHA-1 ハッシュを提供しています。このハッシュを使用すれば、Java Blacklist Jar 機能を介した不正利用を阻止できます。また、シスコでは、デフォルトで感染した *. jar* ファイルをブラックリストに追加するように Java に対して要請しています。この変更は Java SE 8 Update 45 で入手できます。その他の詳細については、このアドバイザリの「回避策」の項を参照してください。

この脆弱性は、Cisco Bug ID CSCup83001（ 登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2015-0691 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

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

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x

CSCup83001 - Cisco Secure Desktop Cache Cleaner Command Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **8.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Workaround		Confirmed	

影響

この脆弱性の利用に成功した攻撃者は、感染した *.jar* ファイルを実行するユーザの特権を使用してクライアント ホスト上で任意のコマンドを実行できます。

ソフトウェア バージョン及び修正

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 Cisco Security Advisories, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

この脆弱性が修正されたソフトウェアは存在しません。感染した *.jar* ファイルを含む Cisco Secure Desktop パッケージはすでに削除されており、ダウンロードできません。

Cisco Secure Desktop をご使用のお客様は、Cisco Host Scan スタンドアロン パッケージに移行する必要があります。

注：Cache Cleaner 機能は 2012 年 11 月から使用が停止されています。追加情報については、下記にてご確認ください。
http://www.cisco.com/c/en/us/td/docs/security/csd/csd36/public_notices/vault_cc_ksl_host_emulation_deprecat_notice.html

この脆弱性は、悪意のある *.jar* ファイルを実行するホストに影響します。Cisco ASA ソフトウェアと Cisco IOS ソフトウェアは、この脆弱性の影響を受けません。

攻撃者はシスコによって署名された *.jar* ファイル内の脆弱性を利用できるため、この脆弱性は Cisco Secure Desktop の使用者だけでなく、任意のユーザに対して利用される可能性があります。

シスコは、感染したバージョンの *.jar* ファイル用の SHA-1 ハッシュを提供しています。このハッシュを使用すれば、Java Blacklist Jar 機能を介した不正利用を阻止できます。また、シスコでは、デフォルトで感染した *. jar* ファイルをブラックリストに追加するように Java に対して要請しています。この変更は Java SE 8 Update 45 で入手できます。その他の詳細については、このアドバイザリの「回避策」の項を参照してください。

回避策

この脆弱性の利用は、*cache.jar* ファイルの実行を阻止することによって回避できます。これは、Java SE 6 Update 14 で導入された Java Blacklist Jar 機能を使用して実現できます。この機能については、Java SE 6 Update 14 のリリース ノート（ http://www.oracle.com/technetwork/java/javase/6u14-137039.html ）を参照してください。

ブラックリストに掲載された *.jar* ファイルは次の SHA-1 メッセージ ダイジェストで確認できます。

```
#Cisco - CSCup83001
mF8yk1Hxc1uH9UorvfG2GJ+ScqY= yUcLgsHB7H6rf04gLNe0ikKrmfI=
UcdnWBajIuVvJjoGHAPA11Gkg7E=
```

シスコでは、Java がこれらのハッシュをデフォルトでブラックリストに追加するようにも要請しています。この変更は Java SE 8 Update 45 で入手できます。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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 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 に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ 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、その会社からシスコ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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、シスコ認定パートナー、リセラー、およびディストリビュータ（認定サードパーティ ベンダー）から購入したものの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 Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +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

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

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、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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不正利用事例とその公表は確認しておりません。

この脆弱性は Jason Sinchak からシスコに報告されたものです。

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。またシスコはいつでも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、単独の転載や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

このアドバイザリは次のリンクにある Cisco Security に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150415-csd

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy の Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.0	2015-April-15	Initial public release.

シスコ セキュリティ手順

シスコ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サポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、Cisco Security Advisory 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。すべてのシスコ 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。

Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses
Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules