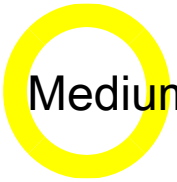
MIT Kerberos GSS-APIライブラリリモートDoS脆弱性



アドバイザリーID : Cisco-SA-20100519-CVE-2010-1321
初公開日 : 2010-05-19 15:40
最終更新日 : 2015-01-31 05:30
バージョン 19.0 : Final
CVSSスコア : 6.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2010-1321
CVE-2010-3566
CVE-2010-3565
CVE-2010-3541
CVE-2010-3563
CVE-2010-3562
CVE-2010-3561
CVE-2010-3560
CVE-2010-3549
CVE-2010-3548
CVE-2010-3569
CVE-2010-3568
CVE-2010-3567
CVE-2010-3555
CVE-2010-3554
CVE-2010-3553
CVE-2010-3552
CVE-2010-3574
CVE-2010-

3551
CVE-2010-3573
CVE-2010-3550
CVE-2010-3572
CVE-2010-3571
CVE-2010-3570
CVE-2010-3559
CVE-2010-3558
CVE-2010-3557
CVE-2010-3556

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

MIT Kerberosには、認証されたリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、ポインタの検証が不十分なため、GSS-APIアクセプタコンポーネントに存在します。 認証されたリモート攻撃者は、該当コンポーネントに対して巧妙に細工された要求を行うことで、この脆弱性を不正利用する可能性があります。 この操作により、コンポーネントがクラッシュし、DoS状態が発生する可能性があります。

MITはこの脆弱性を確認し、更新されたソフトウェアをリリースしました。

この脆弱性は、認証された攻撃者によってのみ不正利用される可能性があり、該当システムへの攻撃の脅威をいくらか軽減できます。

Active Directoryシングルサインオンが有効な場合、Cisco Network Admission Control(NAC)ゲストサーバが影響を受ける可能性があります。

該当製品

MITは次のリンクでセキュリティアドバイザリをリリースしました。MITKRB5-SA-2010-005

シスコは次のリンクでバグIDをリリースしました。CSCtg59379

F5 Networksは、次のリンクのリリースノートで脆弱性を確認しています。Enterprise Manager 2.3.0のリリースノート

HPは次のリンクでセキュリティ情報c02257427をリリースしています。HPSBUX02544 SSRT100107

IBMは次のリンクでセキュリティアラートをリリースしました：CVE-2010-1321

Oracleは次のリンクでセキュリティアラートをリリースしました。Critical Patch Update October 2010

Red Hatはセキュリティアドバイザリを次のリンクでリリースしました： RHSA-2010-0423、RHSA-2010:0770、RHSA-2010:0873、RHSA-2010:0935、RHSA-2010:0987、RHSA-210 152、およびRHSA-2011:0880

Sunは次のリンクでセキュリティ通知をリリースしました。CVE-2010-1321

VMwareは、VMSA-2010-0013、VMSA-2010-0016、およびVMSA-2011-0013の各リンクでセキュリティアドバイザリをリリースしています。

脆弱性のある製品

MIT Kerberos 5バージョン1.8.1以前には脆弱性が存在します。

脆弱性を含んでいないことが確認された製品

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。

回避策

適切なアップデートを適用することを推奨します。

管理者は、信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

影響を受けるアプリケーションへのアクセス権は、信頼できるユーザのみに付与することを推奨いたします。

シスコのお客様は、Cisco

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

MITは次のリンクでパッチをリリースしました。MITKRB5-SA-2010-005

CentOSパッケージは、up2dateコマンドまたはyumコマンドを使用して更新できます。

F5 Networksは、次のリンクで登録ユーザ向けのソフトウェアアップデートをリリースしています。Enterprise Manager 2.3.0

HPは次のリンクでKerberos Web Update(KRB5CLIENT)の更新ソフトウェアをリリースしています。

HP-UX B.11.11(11i v1)
KRB5CLIENT_C.1.3.5.10_HP_UX_B.11.11_32_64.depot以降

HP-UX B.11.23(11i v2)
KRB5CLIENT_D.1.6.2.08_HP_UX_B.11.23_IA_PA.depot以降

HP-UX B.11.31(11i v3)
KRB5CLIENT_E.1.6.2.08_HP_UX_B.11.31_IA_PA.depot以降

HPは、次のリンクで登録ユーザ向けにCore-OS(KRB5-Client)のKerberosクライアント製品用の更新されたソフトウェアをリリースしています。

HP-UX B.11.11(11i v1)
PHSS_41166またはそれ以降

HP-UX B.11.23(11i v2)
PHSS_41167またはそれ以降

HP-UX B.11.31(11i v3)
PHSS_41168またはそれ以降

IBMは次のリンクでアップデートをリリースしています。IBM Developer Kits

Oracleは、登録ユーザ向けのパッチを次のリンクでリリースしました。 Oracle

Red Hatパッケージは、up2dateまたはyumコマンドを使用して更新できます。

Sunは、次のリンクで登録ユーザ向けのパッチをリリースしています。

SPARC
Solaris 10(パッチ141500-07以降)
パッチ112908-38以降が適用されたSolaris 9
パッチ112390-17以降が適用されたSolaris 8

Intel
Solaris 10(パッチ141501-08以降)
パッチ115168-24以降が適用されたSolaris 9
パッチ112240-16以降が適用されたSolaris 8

VMwareは、次のリンクで更新されたソフトウェアをリリースしています。

ESX 3.5
ESX350-201008411-SG

ESX 4.0
ESX400-201009403-SG

ESXi 4.1
ESXi410-201010401-SG

ESX 4.1
ESX410-201010419-SG
ESX410-201110201-SG

ESX 3.0.3
ESX303-201102401-SG

vCenter 4.1
アップデート2

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）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やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20100519-CVE-2010-1321

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリ	適用外	Final	2010年5月

バージョン	説明	セクション	ステータス	日付
	ース			19日

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。