Network Time Protocolデーモン対称モードパケット処理のDoS脆弱性

Medium

アドバイザリーID : Cisco-SA-20150408-CVE-2015-1799 CVE-2015-1799
初公開日 : 2015-04-08 16:41
最終更新日 : 2015-07-23 12:35
バージョン 4.0 : Final
CVSSスコア : 4.3
回避策 : No Workarounds available
Cisco バグ ID : CSCut77471

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

ntpdの脆弱性により、認証されていない隣接する攻撃者が該当システムでサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、対称キー認証の失敗を処理する際のネットワークタイムプロトコル(NTP)パケットの不適切な処理に起因します。攻撃者は、man-in-the-middle（中間者）攻撃を実行して、NTP状態変数が設定された巧妙に細工されたNTPパケットを定期的に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NTPホスト間の通信を中断し、同期を妨げて正当なユーザのDoS状態を引き起こす可能性があります。

NTP.orgは、セキュリティアドバイザリでこの脆弱性を確認し、ソフトウェアアップデートをリリースしました。

この脆弱性を不正利用するには、攻撃者が信頼できる内部ネットワークにアクセスし、巧妙に細工された要求を該当ソフトウェアに送信する必要がある場合があります。このアクセス要件により、エクスプロイトが成功する可能性が制限される可能性があります。

攻撃者は、この脆弱性を不正利用するために、中間者攻撃を実行して巧妙に細工されたパケットをターゲットデバイスに送信しようとする可能性があります。

レポートでは、対称キー認証メカニズムを使用するように設定されたシステムが影響を受けることが示されています。

該当製品

NTP.orgは、次のリンクでバグID Sec 2781のセキュリティ通知をリリースしています。 CVE-2015-1799

シスコは、Bug ID CSCut77422および CSCut77471のセキュリティアドバイザリを次のリンクでリリースしています。 cisco-sa-20150408-ntpd

ICS-CERTは次のリンクで脆弱性に関するノートをリリースしました： CVE-2015-1799

Apple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。HT204942

FreeBSDは次のリンクでVuXMLドキュメントをリリースしました。 ntpの複数の脆弱性

HPは次のリンクでセキュリティ情報c04679309を公開しています。HPSBUX03333 SSRT102029

Red Hatは、バグ1199435に関する公式のCVEステートメントとセキュリティアドバイザリをCVE-2015-1799およびRHSA-2015-1459で公開しています

脆弱性のある製品

4.2.8p2より前のバージョンの ntpd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、管理者ユーザーのみが管理システムまたは管理システムにアクセスすることを許可することを推奨します。

この脆弱性を悪用しようとする攻撃を検出して防止するために、侵入防御システム(IPS)または侵入検知システム(IDS)を実装することをお勧めします。

Cisco Applied Intelligenceチームは、管理者がこの脆弱性を悪用しようとする試みを識別して緩和できるように、関連する次のドキュメントを更新されたソフトウェアの適用前に作成しています。 Identifying and Mitigating Multiple Vulnerabilities in Network Time Protocol

修正済みソフトウェア

NTP.orgは、 ntp 4.2.8p2以降のリンクでソフトウェアアップデートをリリースしています。

契約が有効なシスコのお客様は、 CiscoのSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、次の電子メールを介してアップグレードを入手できます。
tac@cisco.com

Appleは次のリンクで更新されたソフトウェアをリリースしました： OS X Yosemite 10.10.4

FreeBSDは次のリンクからportsコレクションの更新をリリースします。 Ports Collection Index

HPは、セキュリティ情報の「解決策」のセクションで説明されているように、お客様向けに更新されたソフトウェアをリリースしています。

Red Hatは、Red Hat Networkの登録ユーザ向けに更新されたソフトウェアをリリースしました。Red Hatパッケージは、Red Hat Enterprise Linuxバージョン5以降では、yumツールを使用してアップデートできます。

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）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-20150408-CVE-2015-1799

改訂履歴

バージョン	説明	セクション	ステータス	日付
3.0	Appleは、Network Time Protocolデーモン対称モードパケット処理のサービス妨害の脆弱性に対処するために、セキュ	適用外	Final	2015年7月1日

バージョン	説明	セクション	ステータス	日付
	リティアドバイザリをリリースし、ソフトウェアを更新しました。			
2.0	HPは、Network Time Protocol(NTP)デーモン対称モードパケット処理によるサービス妨害の脆弱性に対処するために、セキュリティ情報と更新されたソフトウェアをリリースしました。	適用外	Final	2015年5月21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。