Network Time Protocol（NTP） ServiceÂ 脆弱性のパッケージ RemoteÂ メッセージ ループ否定

Medium	**アドバイザリーID :** Cisco-SA-20091208-CVE-2009-3563 **初公開日 :** 2009-12-08 22:33 **最終更新日 :** 2015-05-12 19:46 **バージョン 20.0 :** Final **CVSSスコア :** 5.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2009-3563

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

ネットワーク タイム プロトコル（NTP）パッケージにより非認証を可能にする可能性があるサービス拒否 （DoS）状態を引き起こすために脆弱性がリモート攻撃者含まれています。

脆弱性はある特定の不正メッセージの処理のエラーが原因です。 非認証は脆弱 な ホストに、リモート攻撃者スプーフィングされたソース IP アドレスの悪意のある NTP パケットを送信 する可能性があります。 ホストがパケットを処理すれば、別の NTP ホストに同じようなパケットを送信 する可能性があります。 この操作はそれらがログファイルに余分な CPU リソースおよびディスクスペース書き込みメッセージを消費します可能性がある両方のホスト間のメッセージ ループを開始する可能性があります。 これら二つの条件により影響を受けたホストの DoS 条件を引き起こす可能性があります。

機能エクスプロイト コードは利用できます。

NTP.org は changelog のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

この脆弱性は 2 つの方法の 1 つで不正利用することができます。 それは NTP を稼動する単一 システムを攻撃し、それにそれ自身にパケットを送信させます使用することができます。 また、それが NTP を稼動する 2 つのシステムを目標とするのに使用できます。 この場合、2 つのシステムは急速に互い間のメッセージをあちこちに送信 しま、メッセージを伝えるために各システムの DoS 条件を引き起こし、またネットワーク帯域幅を消費します。

該当製品

修正済みソフトウェア

NTP バージョン 4.2.4p7 は前に脆弱であり。

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。

改訂履歴

バージョン	説明	Section	ステータス	日付
19.0	HP はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために追加の セキュリティ情報および更新済ソフトウェアをリリースしました。	該当なし	Final	2013-Mar-28
18.0	HP はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために追加の セキュリティ情報および更新済ソフトウェアをリリースしました。	該当なし	Final	2011-Apr-04
17.0	HP はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために追加の セキュリティ情報および更新済ソフトウェアをリリースしました。	該当なし	Final	2010-Oct-06
16.0	VMware はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために Security Advisory を更新済ソフトウェア再リリースし。	該当なし	Final	2010-Jun-28
15.0	VMware はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために Security Advisory および更新済ソフトウェアをリリースしました。	該当なし	Final	2010-Jun-01
14.0	NetBSD はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために Security Advisory およびアップデー	該当なし	Final	2010-Ap

	トされたパッケージをリリースしました。			r-27
13.0	Sun はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために更新済ソフトウェアのアラート 通知を再リリースしました。	該当なし	Final	2010-Apr-14
12.0	HP はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるためにセキュリティ情報および更新済ソフトウェアをリリースしました。	該当なし	Final	2010-Mar-24
11.0	Sun はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるためにアラート 通知および更新済ソフトウェアを再リリースしました。	該当なし	Final	2010-Mar-12
10.0	VMware はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために Security Advisory および更新済ソフトウェアをリリースしました。	該当なし	Final	2010-Mar-05
~9.0	MontaVista ソフトウェアはパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるためにセキュリティ警報および更新済ソフトウェアを再リリースしました。 IBM はまたこの脆弱性に対処するために APAR をリリースしました。	該当なし	Final	2010-Mar-03
8.0	MontaVista ソフトウェアはパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるためにセキュリティ警報および更新済ソフトウェアをリリースしました。	該当なし	Final	2010-Feb-23
7.0	Sun はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるためにアラート 通知および中間セキュリティ救助ソフトウェアをリリースしました。	該当なし	Final	2010-Jan-15
6.0	FreeBSD はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP）当たるために Security Advisory およびアップデートされたパッケージをリリースしました。	該当なし	Final	2010-Jan-

				07
5.0	Nortel はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP） 当たるために更新済ソフトウェアに関するセキュリティ情報を発表しました。 CentOS は脆弱性に対処するために追加更新済パッケージをリリースしました。	該当なし	Final	2009-Dec-21
4.0	CentOS はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP） 当たるために更新済パッケージを再リリースしました。	該当なし	Final	2009-Dec-15
3.0	Cisco は追加製品がパッケージ リモート メッセージ ループ サービス拒否の脆弱性から Network Time Protocol（NTP）影響を受ける確認し、不具合 ID 機能エクスプロイト コードをまた利用できますことを発行しました。	該当なし	Final	2009-Dec-11
2.0	CentOS はパッケージにリモート メッセージ ループ サービス拒否の脆弱性を Network Time Protocol（NTP） 当たるために更新済パッケージをリリースしました。	該当なし	Final	2009-Dec-09
1.0	Network Time Protocol（NTP）パッケージにより非認証を可能にする可能性があるサービス拒否状態を引き起こすために脆弱性がリモート攻撃者含まれています。 更新は利用できます。	該当なし	Final	2009-Dec-08

利用規約