Cisco TelePresenceシステムソフトウェアのコマンド実行の脆弱性

High

アドバイザリーID : cisco-sa-20140122-cts CVE-2014-0661
初公開日 : 2014-01-22 16:00
バージョン 1.0 : Final
CVSSスコア : 8.3
回避策 : No Workarounds available
Cisco バグ ID : CSCui32796

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 TelePresenceシステムソフトウェアの System Status Collection Daemon(SSCD)コードには脆弱性があり、認証されていない隣接する攻撃者が rootユーザの権限で任意のコマンドを実行する可能性があります。

シスコはこ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。この脆弱性を軽減する回避策はありません。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-20140122-cts

該当製品

脆弱性のある製品

この脆弱性は、次のハードウェアで実行されているCisco TelePresence Systemソフトウェアに影響を与えます。

- Cisco TelePresence System 500-32
- Cisco TelePresence System 500-37
- Cisco TelePresence System 1000
- Cisco TelePresence System 1100
- Cisco TelePresence System 1300-65
- Cisco TelePresence System 3000
- Cisco TelePresence システム 3010
- Cisco TelePresence System 3200
- Cisco TelePresence システム 3210

- Cisco TelePresence System TX1300 47（別名TX1300-47）
- Cisco TelePresenceシステム TX1310 65
- Cisco TelePresenceシステムTX9000
- Cisco TelePresenceシステムTX9200

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。

詳細

System Status Collection Daemon(SSCD)コードの脆弱性により、認証されていない隣接する攻撃者がrootユーザの権限で任意のコマンドを実行する可能性があります。

この脆弱性は、XMLリモートプロシージャコール(RPC)を介してSSCDコードに渡されるパラメータの検証が不適切であることに起因します。攻撃者は、巧妙に細工されたXML-RPCメッセージを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はrootユーザの権限を使用して、スタック破損による任意のコールを実行できる可能性があります。

この脆弱性は、Cisco Bug ID CSCui32796(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-2014-0661が割り当てられています。

回避策

この脆弱性を軽減する回避策はありません。

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。

次の表に、該当製品のCisco TelePresenceシステムソフトウェアの最初の修正リリースに関する情報を示します。

製品	First Fixed Release（修正された最初のリリース）
Cisco TelePresence System 500-32	6.0.4(11) 以降

Cisco TelePresence System 500-37	1.10.2(42) 以降
Cisco TelePresence System 1000	1.10.2(42) 以降
Cisco TelePresence System 1300-65	1.10.2(42) 以降
Cisco TelePresence System 3000	1.10.2(42) 以降
Cisco TelePresence システム 3010	1.10.2(42) 以降
Cisco TelePresence System 3200	1.10.2(42) 以降
Cisco TelePresence システム 3210	1.10.2(42) 以降
Cisco TelePresence System 1300-47	6.0.4(11) 以降
Cisco TelePresenceシステムTX1310 65	6.0.4(11) 以降
Cisco TelePresenceシステムTX9000	6.0.4(11) 以降
Cisco TelePresenceシステムTX9200	6.0.4(11) 以降

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。

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140122-cts

改訂履歴

リビジョン 1.0	2014年1月22日	初版リリース

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。