Cisco StarOS CLI Command Injection Vulnerability

High

アドバイザリーID : cisco-sa-20170705-asrcmd
初公開日 : 2017-07-05 16:00
バージョン 1.0 : Final
CVSSスコア : 8.2
回避策 : No workarounds available
Cisco バグ ID : CSCvc69329 CSCvc72930

CVE-2017-6707

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 ASR 5000 シリーズ、5500 シリーズ、および 5700 シリーズ デバイス用 Cisco StarOS オペレーティング システムおよび Cisco Virtualized Packet Core（VPC）ソフトウェアの CLI コマンド解析コードの脆弱性により、認証されたローカル攻撃者が該当システムの StarOS CLI から侵入して、システムの Linux *root* ユーザとして任意のシェル コマンドを実行する可能性があります。

この脆弱性は、該当オペレーティング システムがコマンドを十分にサニタイズせずに Linux シェル コマンドに挿入することに起因します。 攻撃者は、Linux シェルコマンドで実行されるよう、巧妙に細工した CLI コマンドを *root* ユーザとして送信することで、この脆弱性を不正利用する可能性があります。 不正利用に成功すると、攻撃者は StarOS CLI から侵入して、Linux *root* ユーザとして該当システムの任意のコマンドを実行する可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-asrcmd

該当製品

脆弱性のある製品

この脆弱性は Cisco StarOS オペレーティング システムを実行する次のシスコ製品に影響を与えます。

- ASR 5000 シリーズ
- ASR 5500 シリーズ
- ASR 5700 シリーズ
- Virtualized Packet Core-Distributed Instance（VPC-DI）ソフトウェア
- Virtualized Packet Core-Single Instance（VPC-SI）ソフトウェア

脆弱性のある Cisco StarOS リリースが Cisco ASR 5000 / 5500 / 5700 シリーズ デバイスで実行されているかどうかを確認するには、デバイスの CLI で **show version** コマンドを使います。 次の例は、Cisco StarOS リリース 19.2.1 を実行する Cisco ASR 5500 シリーズ ルータでのコマンドの出力を示しています。

```
[local]ASR-2# show version

Friday August 12 13:17:31 AST 2016
Active Software:
 Image Version:                 19.2.1
 Image Build Number:            62564
 Image Description:             Deployment_Build
 Image Date:                    Thu Dec 31 20:13:39 EST 2015
 Boot Image:                    /flash/asr5500-19.2.1.bin
```

脆弱性のある Cisco StarOS リリースが VPC-SI または VPC-DI インスタンスで実行されているかどうかを確認するには、デバイスの CLI で **show version** コマンドを使います。 次の例は、Cisco StarOS リリース 20.1.v0（VPC-DI リリース N4.6）を実行している VPC-DI インスタンスでのコマンドの出力を示しています。

```
[local]VPC-DI# show version

Active Software:
 Image Version:                 20.1.v0
 Image Build Number:            64657
 Image Description:             Deployment_Build
 Image Date:                    Wed Jul 27 18:46:53 EDT 2016
 Boot Image:                    /flash/qvpc-di-20.1.v0.bin
```

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。

シスコは、この脆弱性が Cisco Elastic Services Controller（ESC）および Cisco Ultra Automation Services（UAS）には影響を与えないことを確認しました。

詳細

攻撃者はこの脆弱性を不正利用するため、Cisco StarOS CLI コマンドのいずれかを使用します。しかし、攻撃者はまずコンソールまたはセキュア シェル（SSH）で非管理者ユーザとして該当デ

バイスに認証される必要があります。 正常に認証されるため、攻撃者はそのデバイスに存在する侵害された非管理者ユーザ アカウントを使用します。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

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。 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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載された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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける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。

サービス契約をご利用でないお客様

シスコから直接購入したが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、サードパーティ ベンダーから購入したが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 TAC に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

修正済みリリース

このセクションの表を参考に、適切な修正済みリリースにアップグレードする必要があります。

Cisco ASR 5000 シリーズ、5500 シリーズ、および 5700 シリーズ デバイス

次の表では、最初の列に、Cisco StarOS オペレーティング システムのメジャー リリースを示します。 2 番目の列には、本脆弱性の修正を含んだ最初のマイナー リリースを示します。

Cisco StarOS Major Release	First Fixed Release (修正された最初のリリース)
18.0	18.7.6
19.0	19.6.5
20.0	20.2.9
21.0	21.1.1

Cisco Virtualized Packet Core ソフトウェア

次の表では、最初の列に Cisco Virtualized Packet Core (VPC) ソフトウェアのメジャー リリース、およびカッコ内に関連付けられた Cisco StarOS オペレーティング システムのリリースを示します。 2 番目の列には、本脆弱性の修正を含んだ Cisco VPC ソフトウェアの最初のマイナー リリースを示します。

Cisco VPC Software and Cisco StarOS Major Release	First Fixed Release (修正された最初のリリース
N4.0 (19.2)	5.0.3 or 5.1
N4.2 (19.3)	5.0.3 or 5.1
N4.5 (20.0)	5.0.3 or 5.1
N4.6 (20.1)	5.0.3 or 5.1
N4.7 (20.2)	5.0.3 or 5.1
N5.0 (21.0)	5.0.3

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エクスプロイト事例やその公表を確認していません。

出典

この脆弱性はサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-asrcmd

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-July-05

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。