Cisco Nexus シリーズ スイッチ Telnet CLI コマンド インジェクト脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170517-nss1 **初公開日 :** 2017-05-17 16:00 **最終更新日 :** 2017-07-05 20:27 **バージョン 1.1 :** Final **CVSSスコア :** 4.4 **回避策 :** Yes **Cisco バグ ID :** CSCvb86771	CVE-2017-6650

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

on Cisco Nexus シリーズ スイッチを実行する Cisco NX-OS システム ソフトウェアの Telnet CLI コマンドの脆弱性はコマンド インジェクト 攻撃を行う認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性はコマンド ライン引数の不十分な入力の検証が原因です。 攻撃者は Telnet CLI コマンドに細工 された コマンド 引数をインジェクトすることによってこの脆弱性を不正利用する可能性があります。 エクスプロイトはユーザのユーザのパスの外の特権レベルで read または write 任意ファイルに攻撃者を可能にする可能性があります。

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。
517-nss1

影響を受ける製品

脆弱性が存在する製品

この脆弱性はデフォルト 設定で動作する次の Cisco Nexus シリーズ スイッチに影響を与えます。

Cisco Nexus 3000 Series Switches

Cisco Nexus 3500 プラットフォーム スイッチ
Cisco Nexus 5000 Series Switches
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9500 R シリーズ スイッチ
Cisco Nexus 9000 シリーズ スイッチ-スタンドアロン、NX-OS モード
Cisco MDS 9000 Series Multilayer Switches

該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

脆弱性が存在しない製品

Cisco Nexus 9000 シリーズ ファブリックスイッチ- ACI モード

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。

細部

回避策

この脆弱性に対処する回避策はありません。

固定ソフトウェア

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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、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。

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。

ソース

この脆弱性は内部 保全テストの間に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss1

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	脆弱性が存在する製品の更新済リスト。	脆弱性のある製品	最終版	2017-July-05
1.0	初回公開リリース		最終版	2017-May-17

利用規約