CiscoSecure ACS for Windows NT Serverの複数の脆弱性

アドバイザリーID : cisco-sa-20000921-secure-acs-nt
初公開日 : 2000-09-21 17:00
バージョン 1.3 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

CiscoSecure ACS for Windows NT Serverでは、次の複数の脆弱性が確認され、修正されています。

- CSAdminソフトウェアモジュールは、サイズの大きいURLを送信することで強制的にクラッシュさせることができます。この不具合は、Cisco Bug ID CSCdr68286に記載されています。
- CiscoSecure ACS for Windows NT Serverは、サイズが大きすぎるTACACS+パケットを送信することで、不安定な状態になることがあります。この不具合は、Cisco Bug ID CSCdr51286に記載されています。
- CiscoSecure ACS for Windows NT Serverを、ユーザがヌルパスワードを使用できるLDAPサーバと組み合せて使用している場合は、イネーブルパスワードをバイパスして、ルータまたはスイッチ上で不正な特権を取得できます。この不具合は、Cisco Bug ID CSCdr26113に記載されています。

CiscoSecure ACS for Windows NT Serverの2.1(x)、2.3(3)、2.4(2)までのリリースには脆弱性が存在します。これらの不具合は、リリース2.4(3)以降のすべてのリリースで修正されています。次に示すように、該当するすべてのカスタマーに無償アップグレードが提供されます。アップグレードの代わりに、これらの不具合による脅威を最小限に抑える複数の回避策があります。

CiscoSecure ACS for UNIXは、これらの脆弱性の影響を受けません。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20000921-secure-acs-ntで確認できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

このドキュメントで説明する不具合は、CiscoSecure ACS for Windows NT Serverのリリース2.1(x)、2.3(3)、および2.4(2)と、それ以前のすべてのリリースに存在します。

リリース2.4(3)では、これら3つの不具合はすべて修復されています。これ以降のCiscoSecure ACS for Windows NT Serverリリースにはすべて、この修正が含まれます。

脆弱性を含んでいないことが確認された製品

前述のCiscoSecure ACSリリースは、Windows NT Serverで実行されている場合にのみ脆弱です。CiscoSecure ACS for UNIXは、これらの脆弱性が原因で特に危険にさらされることはありません。

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

0.CSCdr68286

CSAdminモジュール内のバッファオーバーフロー状態は、サイズの大きいパケットをCiscoSecure ACS Server for Windows NTのTCPポート2002に送信することによって不正利用できます。基盤となるNTオペレーティングシステムの正確なバージョンによっては、挿入されたコードを強制的に実行したり、モジュールを一時的にクラッシュさせたりする可能性があります。クラッシュが発生すると、既存の管理セッションはすべて終了し、最新の管理操作が失われる可能性があります。バージョン2.3(x)以降では、CSAdminモジュールは1分以内に自動的に再起動されます。その時点で既存のセッションは再確立されますが、最初から開始されたかのように、は再度認証される必要があります。以前のバージョンでは、サーバを再起動する必要があります。

この脆弱性は認証なしでトリガーされる可能性がありますが、通常は想定されるすべてのアクティビティに認証が必要です。

0.CSCdr51286

サイズが大きすぎるTACACS+パケットをCiscoSecure ACS for Windows NT Serverに送信することで、システムがサービス拒否の原因となる不安定な状態になる可能性があります。この脆弱性を不正利用するには、攻撃者はTACACS+クライアントとCiscoSecure ACS for Windows NT Server間のパスをスニッフィングするか、トラフィックを注入できる必要があります。

0.CSCdr26113

一部のLightweight Directory Access Protocol(LDAP)サーバでは、ユーザが未定義のパスワードを設定できます。これは、保存されたパスワードの値がnullであることを意味します。このようなLDAPサーバとこの不具合間のインタラクションにより、特権モードの有効なパスワードを指定しなくても、イネーブルモード認証が成功する可能性があります。

回避策

次の回避策は、これらの不具合に起因する脅威の軽減に役立ちますが、脆弱性が悪用される可能性を完全に排除することはできません。該当するシステムをご使用のお客様には、このセキュリティアドバイザリで前述されている、該当しない修正済みバージョンのソフトウェアにアップグレードすることを強くお勧めします。ソフトウェアのアップグレードの代わりに、次の手順がリスクを最小限に抑えるのに役立ちます。

0.CSCdr68286

サイズが大きすぎるURLからCSAdminモジュールを保護するには、CiscoSecure ACSサーバへのアクセスを制限して、正当なニーズを持つコンピュータだけがネットワーク経由でサーバに到達できるようにします。これは、CiscoSecure ACSサーバとネットワークの残りの部分との間のルータにアクセスコントロールリスト(ACL)を配置することで実現できます。次の例では、CiscoSecure ACSサーバのIPアドレスは1.1.1.1で、隣接ルータのEthernet0インターフェイスに接続されています。ターミナルサーバのアドレスは2.2.2.2です。ターミナルサーバとCiscoSecure ACSサーバの間のアクセスは、イネーブルモードからconfigモードに入り、次の手順のリストのようなコマンドを使用してACLを作成し、ルータのEthernet0インターフェイスに適用することで防止できます。

<#root>

```
access-list 200 permit ip host 2.2.2.2 host 1.1.1.1 eq 49
    access-list 200 deny any any log

    interface Ethernet0
    ip access-group 200 incoming
```

0.CSCdr51286

CiscoSecure ACSサーバをオーバーサイズのTACACS+パケットの受信から保護するには、上に示すように隣接ルータにACLを適用するか、ACSを保護ネットワークの一部と見なすファイアウォールデバイスにアクセスコントロールを実装します。

別の方法として、CiscoSecure ACS for Windows NT Serverと、それを使用しているデバイスとの間に信頼できるパスが存在することを確認する方法もあります。これは、そのパスに沿ったパケットのスニッフィングやインジェクトを防止するための慎重な対策です。

0.CSCdr26113

この不具合による不正なイネーブルアクセスは、リモートLDAPサーバではなくCiscoSecure ACS for Windows NTサーバ自体にイネーブルパスワードを直接保存することで阻止できます。

修正済みソフトウェア

リリース2.4(3)より前のすべてのバージョンのCiscoSecure ACS for Windows NT Serverは、これら3つの脆弱性の影響を受けます。リリース2.4(3)より前のバージョンを使用している場合は、2.4.(3)以降にアップグレードする必要があります。

CiscoSecure ACS for UNIXの任意のバージョンを実行しているお客様には、このセキュリティアドバイザリに記載されている不具合の脆弱性はありません。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20000921-secure-acs-nt

改訂履歴

リビジョン 1.3	2000年 10月20日	修正済みソフトウェアを入手するためにTACに問い合わせるように顧客に求めるように編集。
リビジョン 1.2	2000年 9月21日	初回公開リリース

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。