Cisco VPN 3000 コンセントレータ 多重 脆弱点

severity

アドバイザリーID : cisco-sa-20020903-vpn3k-vulnerability

初公開日 : 2002-09-03 15:00

バージョン 2.0 : Final

回避策 : Yes

Cisco バグ ID :

CVE-2001-0554

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 VPN 3000 シリーズ コンセントレータはデータ暗号化のための特別な目的のために建てられた、リモート アクセス バーチャル プライベート ネットワーク （VPN）プラットフォームおよび認証の系列です。

このアドバイザリは Cisco VPN 3000 シリーズ コンセントレータおよび Cisco VPN 3002 Hardware Client のための多重 脆弱点を文書化します。 これらの脆弱性は Cisco バグ ID の CSCdt56514、CSCdu15622、CSCdu35577、CSCdu82823、CSCdv66718、CSCdv88230、CSCdw22408、CSCdw50657、CSCdx07754、CSCdx24622、CSCdx24632、CSCdx39981、CSCdx54675 および CSCdy38035 として文書化されています。 、バージョン 3.5.5 または 3.6.1 は Cisco VPN 3000 シリーズ コンセントレータおよび Cisco VPN 3002 Hardware Client のためのコードのバージョンにアップグレードしてこれらの文書化された脆弱性すべてから、保護します。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020903-vpn3k-vulnerability で掲示されます。

該当製品

修正済みソフトウェア

Cisco VPN 3000 シリーズ コンセントレータはこれらの脆弱性から影響を受けます。 このシリーズはモデル 3005、3015、3030、3060、3080 および Cisco VPN 3002 Hardware Client が含まれています。

DDTS - 説明	該当するリリース

CSCdt56514 - PPTP、IPSEC 内部 認証ログイン脆弱性	• 3.6 (Rel) • 3.5(Rel) から 3.5.4 • 先により 3.1.2 • 先により 3.0.3 (B) • 2.x.x
CSCdu15622 - HTML パーサー処理の脆弱性	• 先により 3.0.3 (B) • 2.x.x
CSCdu35577 -コンセントレータはアプリケーション層バナーのたくさんの情報を与えます	• 3.5.4 より前 • 3.1.x • 3.0.x • 2.x.x
CSCdu82823 - BSDソース の telnetd の 脆弱性	• 先により 3.0.4 • 2.x.x
CSCdv66718 - Windows PPTP クライアントの脆弱性	• 先により 2.5.2 (F)
CSCdv88230、CSCdw22408 - HTML ビュー出典脆弱性と目に見えるユーザパスワード	• 先により 3.5.1 • 先により 3.1.4 • 3.0.x • 2.x.x
CSCdw50657 - HTML ビュー出典脆弱性と目に見える証明書パスワード	• 先により 3.5.2 • 3.1.x • 3.0.x • 2.x.x

CSCdx07754 - XML パブリックルールの脆弱性	• 先により 3.5.3 • 3.1.x • 3.0.x • 2.x.x
CSCdx24622 - HTML ページ アクセスの脆弱性	• 先により 3.5.3 • 3.1.x • 3.0.x • 2.x.x
CSCdx24632 - HTML ログオン処理の脆弱性	• 先により 3.5.3 • 3.1.x • 3.0.x • 2.x.x
CSCdx39981 - VPN クライアント 認証脆弱性	• 3.6 (Rel) • 先により 3.5.5 • 3.1.x • 3.0.x • 2.x.x
CSCdx54675 - LAN間IPSECトンネルの脆弱性	• 3.5.4 より前 • 3.1.x • 3.0.x • 2.x.x
CSCdy38035 - ISAKMPパケット処理の脆弱性	• 3.6 (Rel) • 先により 3.5.5 • 3.1.x • 3.0.x • 2.x.x

Cisco VPN 3000 シリーズ コンセントレータが影響を受けたソフトウェアを実行したかどうか確認するために、Webインターフェイスか Console メニューによってソフトウェアリビジョンをチェックして下さい。

脆弱性を含んでいないことが確認された製品

これらの脆弱性は VPN Client ソフトウェア Cisco VPN 5000 シリーズ コンセントレータに影響を与えません。 その他のCisco製品はこれらの脆弱性から影響を受けるために知られていません。

改訂履歴

Revision 2.0	2002-September-03	修正された一般公開
リビジョン 1.0	2002-September-03	初版リリース

利用規約