CBOS におけるその他の脆弱性

severity

アドバイザリーID : cisco-sa-20010522-cbos

初公開日 : 2001-05-22 15:00

バージョン 1.1 : Final

回避策 : Yes

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

多重 脆弱点は CBOS で、ルータの Cisco 600 ファミリー用のオペレーティング システム特定および解決されました。

- Cisco CBOS ソフトウェアはその欠陥が割り当て TCP 最初のシーケンス番号の正常な予測含まれています。 それは影響を受けた Ciscoデバイス自体で起きるか、または終端させる TCP 接続のセキュリティだけに影響を与えます; それは 2 つの他のホストの間で影響を受けたデバイスを通して送信中に転送される TCPトラフィックに適用しません。
  この脆弱性は Cisco バグ ID **CSCds16078** として文書化されています。
- Cisco 600 ルータは IP Record Route オプションのエコー要求パケットがそれを通してルーティングされるときトラフィックを通過させることをおよびコンソールに応答することを止めるかもしれません。
  この脆弱性は Cisco バグ ID **CSCds30150** として文書化されています。
- パスワードは、exec およびイネーブル、NVRAM のクリアテキストで保存されます。
  この脆弱性は Cisco バグ ID **CSCdt04882** として文書化されています。
- 多重場合の、大きいエコーリプライパケットは影響を受けた Cisco 600 ルータを通してルーティングされます、ROMMON モードを開始し、それ以上のトラフィックを通過させることを止めます。
  この脆弱性は Cisco バグ ID **CSCds74567** として文書化されています。

CBOS の次のリリースは述べられた脆弱性がすべてが含まれています: 2.0.1、2.1.0、2.1.0a、2.2.0、2.2.1、2.2.1a、2.3、2.3.2、2.3.5、2.3.7 および 2.3.8。

これらの脆弱性は次の CBOS リリースで解決されます: 2.3.9、2.4.1 および 2.4.2。 下記のセクション ソフトウェア バージョン および 修正の詳細に示すように脆弱ではない顧客はリリースにアップグレードするように勧められます。

このアドバイザリは 522-cbos で利用できます。

該当製品

修正済みソフトウェア

影響を受けたモデルは次のとおりです: 627、633、673、675、675E、677、677i および 678。

これらのモデルは次のいずれかを実行すれば脆弱、またはそれ以前、CBOS リリースです: 2.0.1、2.1.0、2.1.0a、2.2.0、2.2.1、2.2.1a、2.3、2.3.2、2.3.5、2.3.7 および 2.3.8。

これらの脆弱性は次の CBOS リリースで解決されます: 2.3.9、2.4.1 および 2.4.2。

脆弱性を含んでいないことが確認された製品

CBOSソフトウェアの他のリリースはこれらの脆弱性から影響を受けしません。 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。

改訂履歴

リビジョン 1.1	2001-July-26	リストに分けられるの代りにテキスト段落内の TAC 連絡先を含める変更された修正済みソフトウェア取得のセクション。 無償ソフトウェアアップグレードについてのその同じセクションの削除された行。
リビジョン 1.0	2001-May-22	初回公開リリース

利用規約