セキュリティ情報（2004年4月28日）

SANRISE9500V/1000シリーズにおけるTCPプロトコルの脆弱性対策について

2004年4月28日
（株）日立製作所RAIDシステム事業部

1. SANRISE9500V/1000シリーズに対するTCPプロトコルの脆弱性対策のお知らせ

インターネット等で広く利用されているTCPプロトコルの脆弱性に関して、下記の情報が公開されました。

NISCC Vulnerability Advisory 236929

http://www.uniras.gov.uk/vuls/2004/236929/index.htm
http://www.jpcert.or.jp/at/2004/at040003.txt

弊社のSANRISE9500V/1000シリーズでは、そのサブシステム管理のためにLAN経由の接続が可能となっております。
この脆弱性を利用した攻撃を受けた場合、影響を受ける危険性がございます。
サブシステム管理機能は直接ストレージ機能には係わりませんので、万一影響を受けましてもストレージとしてのデータの内容およびRead/Write機能には支障はございません。またSANRISEに蓄積されているデータを読み取られることもございません。
しかしながら今後、この脆弱性を利用した攻撃が頻発した場合には、装置の遠隔監視が妨げられたり、設定変更に支障をきたす等の可能性があります。
そのため今般、対象となる製品に対しまして、予防処置をさせていただきます。

2. 今回のTCPプロトコルの脆弱性の特徴

TCPでは、偽造されたTCPセグメントによって通信中のセッションが切断されたり、データの挿入が行われる可能性があります。
今回の場合、インターネット等で広く利用されているTCPに脆弱性が存在するため、攻撃者がこれを利用すれば、ネットワークに接続しているだけで攻撃を受ける可能性があります。

3. 対象製品

SANRISE9580V/9570V/9530V、SANRISE1200/1100

4. 対象となる装置の構成条件

装置がLANに接続され、そのLANを介したネットワーク上でこの脆弱性を利用した攻撃が実行された場合。

5. 対応の内容

本件への対策を施したマイクロコードを準備いたします。本マイクロコードを装置に適用する対策作業は弊社保守員が実施させていただきます。
つきましては弊社までお問い合わせください。

更新履歴

2004年4月28日　調査中を対策済み情報に更新
2004年4月23日　新規情報掲載

本件に関する問合せ窓口
（株）日立製作所RAIDシステム事業部 販売推進本部 販売企画部

問い合わせ先はこちら

ページの先頭へ