

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、設定変更を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](#)

*1 弊社では、セキュリティ対応に関して正確な情報を提供できるよう努力しておりますが、セキュリティ問題に関する情報は変化しており、当ホームページに記載している内容を予告なく変更することがありますので、あらかじめご了承ください。情報ご参照の際には、常に最新の情報をご確認いただくようお願いいたします。

*2 当ホームページに記載されている製品には、他社開発製品が含まれております。これらのセキュリティ情報については他社から提供、または公開された情報を基にしております。弊社では、情報の正確性および完全性について注意を払っておりますが、開発元の状況変化に伴い、当ホームページの記載内容に変更が生じることがあります。

*3 当ホームページはセキュリティ情報の提供を目的としたものであり、法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして、弊社では責任を負いかねます。

[ページの先頭へ](#)

[サイトの利用条件](#) | [個人情報保護に関して](#) | [商品名称について](#) | [更新履歴](#)

© Hitachi, Ltd. 1994, 2022. All rights reserved.