セキュリティ情報（2004年2月13日）

SANRISE9900V/9900V-e、H1024/128におけるSVPセキュリティホール（MS04-007）対策について

2004年2月13日
（株）日立製作所RAIDシステム事業部

1. SANRISE9900Vに対するセキュリティホール対策のお知らせ

Windows NT4.0/2000/XPおよびWindows Server 2003に対する新たなセキュリティホールが公開されました。新たに報告されたセキュリティホールの中で以下のものがSANRISE9900Vシリーズに関係します。

1. MS04-007：ASN.1の脆弱性により、コードが実行される（828028）

現在までのところ、この脆弱性を利用したVirusならびにWormは発見されておらず、またこの脆弱性を突いた攻撃による被害は報告されていません。

弊社のSANRISE9900Vシリーズでは、そのサブシステム管理装置（SVP）としてWindows2000を搭載しているため、今回のセキュリティホールの対象となります。
ただし、SVPは直接ストレージ機能には係わりませんので、万一攻撃者から攻撃された場合であってもストレージとしてのデータの内容およびRead/Write機能に支障はありません。またSANRISEに蓄積されているデータを読み取られることもありません。
しかしながら万一攻撃者によりSVPで任意のコードが実行された場合、装置の構成変更設定や保守作業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. 今回のセキュリティホールの特徴

今回のセキュリティホールでは、ASN.1（Abstract Syntax Notation 1）を使用するためのライブラリにバッファオーバーフローの脆弱性が存在します。攻撃者はこのセキュリティホールを悪用し、対象となるコンピュータ上でシステム特権を用いて任意のコードを実行する可能性があります。

（ASN.1はデータの標準を定義する言語であり、多くのアプリケーションおよびデバイスにより使用されています。ASN.1の詳細についてはマイクロソフト社の情報を参照ください。）

3. 対象製品

SANRISE9980V/9970V、SANRISE9980V-e/9970V-e、SANRISE H1024/ H128

注 :SANRISE9500Vシリーズ、SANRISE 2000/2000-e/1000シリーズ、およびSANRISE H512/H48は影響を受けません。

4. 対象となる装置の構成条件

SVPが装置外部のLANに接続されており、攻撃者が細工を施したデータをSVPに送信可能な環境。

5. 対策の内容

次の対策作業を、弊社保守員が実施させていただきます。
マイクロソフト社より提供されている対策パッチを搭載します。
本パッチにより今回問題となっている脆弱性はカバーされます。

6. Worm/ Virusに対するSANRISEの見解

今回のようにネットワーク接続だけで感染する等、通常のSANRISEの運用でも感染する危険性を持つセキュリティホールが顕在化した場合には、Virus/Wormの出現を待つまでもなく、逐次その旨お知らせすると共に、対策を施させていただきます。
情報の提供はご覧のWebへ掲載する他、サポート契約に基づくSoftware Support Newsにてお知らせいたします。

7. Remote Console Storage Navigatorのご使用について

Remote Console Storage Navigatorを使用されている場合、クライアントPCがWindows NT4.0/2000/XPおよびWindows Server 2003であれば同様の対策が必要と思われます。
詳しくはメーカにお尋ねいただくか、以下のセキュリティサイトをご確認の上対応をお願い致します。

http://www.microsoft.com/japan/

本セキュリティホールに関する情報

http://www.microsoft.com/japan/technet/security/bulletin/ms04-007.mspx

---

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す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、当ホームページで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ない、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

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