セキュリティ情報（2004年4月16日）

SANRISE9900V/9900V-e、H1024/128におけるSVPセキュリティホール（MS04-011～MS04-014）対策について

2004年4月16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

Microsoft製品に対して、以下に示すセキュリティホールが公開されました。

1. MS04-011：Microsoft Windowsのセキュリティ修正プログラム（835732）
2. MS04-012：Microsoft RPC/DCOM用の累積的な修正プログラム（828741）
3. MS04-013：Outlook Express用の累積的な修正プログラム（837009）
4. MS04-014：Microsoft Jetデータベースエンジンの脆弱性によりコードが実行される（837001）

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を搭載しており、上記1および2の脆弱性の影響を受けます。上記3および4については、SVPはサブシステム管理専用装置であるため、本脆弱性に関連したアプリケーションソフトが実行されることはなく、脆弱性の影響は受けません。

現在までのところ、これらの脆弱性を利用したVirusならびにWormは発見されておりませんが、今後この脆弱性を利用したVirusあるいはWormが広まった場合、SVPが攻撃の対象となる危険性があります。
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SVPが攻撃された場合、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

Windowsにデフォルトでインストールされるいくつかの機能／サービスにバッファオーバランの脆弱性が存在します。攻撃者がこの脆弱性を利用すれば、攻撃対象となるコンピュータ上で任意のプログラムの実行が行なわれる可能性があります。

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、そのLANを介したネットワーク上にこの脆弱性を対象としたVirus/Wormに感染したPCが接続された場合。

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（KB835732およびKB828741）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WindowsNT4.0/2000/XP/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/ms04-011.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-012.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-013.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-014.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