セキュリティ情報（2004年12月17日）

SANRISEシリーズにおけるSVPセキュリティホール（MS04-041～045）対策について

2004年12月17日
（株）日立製作所RAIDシステム事業部

1. SANRISEシリーズ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. MS04-041：WordPadの脆弱性により、コードが実行される（885836）
2. MS04-042：DHCPの脆弱性により、リモートでコードが実行され、サービス拒否が起こる（885249）
3. MS04-043：ハイパーターミナルの脆弱性により、コードが実行される（873339）
4. MS04-044：WindowsカーネルおよびLSASSの脆弱性により、特権の昇格が起こる（885835）
5. MS04-045：WINSの脆弱性により、リモートでコードが実行される（870763）

弊社のSANRISEシリーズのSVPにおける、上記1～5の脆弱性の影響は下記の通りです。

1. 本件は、WordPadの脆弱性により、リモートでコードが実行されるというものです。
   攻撃者がこの脆弱性を悪用するには、特別な細工が施されたファイルを作成し、この細工されたファイルをWordPadで開くように、SVP使用者（保守員）を誘導する必要が有ります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
2. 本脆弱性の影響を受けるOSは、Windows NT Server 4.0です。
   弊社のSANRISEシリーズのSVPではWindows NT Server 4.0は使用していないため、本脆弱性の影響は受けません。
3. 本件は、ハイパーターミナルの脆弱性により、リモートでコードが実行されるというものです。
   攻撃者がこの脆弱性を悪用するには、特別な細工が施されたハイパーターミナルセッションファイルを作成し、この細工されたファイルでハイパーターミナルを実行する、あるいは、特別な細工が施されたWebページまたは電子メールメッセージを表示させるように、SVP使用者（保守員）を誘導する必要が有ります。SVPはサブシステム管理専用装置であり、このような操作が行われることはありません。このため、SVPでは本脆弱性の影響は受けません。
4. 本件は、WindowsカーネルおよびLSASSの脆弱性により、ローカルでログオンしているユーザの特権を昇格できるというものです。
   攻撃者がこの脆弱性を悪用するには、対象となるPC上で特別に細工を施したプログラムを実行する必要があります。SVPはサブシステム管理専用装置であるため、このようなプログラムが実行されることはありません。このため、SVPでは本脆弱性の影響は受けません。
5. 本脆弱性の対象OSはWindows NT Server 4.0、Windows 2000 Server、Windows Server 2003です。
   弊社のSANRISEシリーズのSVPではこれらのOSは使用していないため、本脆弱性の影響は受けません。

よって、今回公開された脆弱性については特に対策の必要はありません。

2. 対象製品

Hitachi Universal Storage Platform、Hitachi Universal Storage Platform H12000、
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。

3. Storage Navigatorのご使用について

Storage Navigatorのご使用については、Storage Navigator機能に限ったご使用であれば特に問題ありません。
クライアントPCを他の用途でもご利用されている場合、ご利用内容によっては今回の脆弱性の影響を受ける可能性があります。
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/ms04-041.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-042.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-043.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-044.mspx

http://www.microsoft.com/japan/technet/security/bulletin/ms04-045.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