セキュリティ情報（2005年4月15日）

SANRISEシリーズにおけるSVPセキュリティホール（MS05-016～023）対策について

2005年4月15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. MS05-016：Windowsシェルの脆弱性により、リモートでコードが実行される（893086）
2. MS05-017：メッセージキューの脆弱性により、コードが実行される（892944）
3. MS05-018：Windows Kernelの脆弱性により、特権の昇格およびサービス拒否がおこる（890859）
4. MS05-019：TCP/IP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（893066）
5. MS05-020：Internet Explorer用の累積的なセキュリティ更新プログラム（890923）
6. MS05-021：Exchange Serverの脆弱性により、リモートでコードが実行される（894549）
7. MS05-022：MSN Messengerの脆弱性により、リモートでコードが実行される（896597）
8. MS05-023：Microsoft Wordの脆弱性により、リモートでコードが実行される（890169）

弊社のSANRISEシリーズのSVPにおける、上記1～8の脆弱性の影響は下記の通りです。

1. 本件は、Windowsシェルの脆弱性により、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ファイルを開くように、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. 本件は、メッセージキューのコンポーネントの脆弱性により、リモートでコードが実行されるというものです。
   SVPにはメッセージキューのコンポーネントがインストールされていないため、本脆弱性の影響は受けません。
3. 本件は、下記に示す脆弱性により、特権の昇格およびサービス拒否がおこるというものです。
   a. フォントの脆弱性（CAN-2004-0060）
   b. Windowsカーネルの脆弱性（CAN-2005-0061）
   c. オブジェクト管理の脆弱性（CAN-2005-0550）
   d. CSRSSの脆弱性（CAN-2005-0551）
   攻撃者が上記の脆弱性を悪用するには、対象となるコンピュータにログオンし、特別な細工が施されたアプリケーションを実行するように、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、下記に示すTCP/IPの脆弱性により、リモートからのコードの実行やサービス拒否が起こるというものです。
   a. IPの検証の脆弱性（CAN-2005-0048）
   b. ICMPの接続リセットの脆弱性（CAN-2004-0790）
   c. ICMPのパスMTUの脆弱性（CAN-2004-1060）
   d. TCP接続リセットの脆弱性（CAN-2004-0230）
   e. 詐称の接続要求の脆弱性（CAN-2005-0688）
   上記の脆弱性は、Windows 2000、Windows XP、Windows Server 2003が対象となります。弊社のHitachi Universal Storage PlatformおよびHitachi Universal Storage Platform H12000では、SVPのOSとしてWindows XPを使用しています。また、SANRISE9900VシリーズおよびSANRISE H1024/128では、SVPのOSとしてWindows 2000を使用しています。このため、SVPは本脆弱性の影響を受けます。
5. 本件は、Internet Explorerの下記に示す脆弱性により、リモートでコードが実行されるというものです。
   a. DHTMLオブジェクト メモリの破損の脆弱性（CAN-2005-0553）
   b. URL解析 メモリ破損の脆弱性（CAN-2005-0554）
   c. コンテンツアドバイザ メモリ破損の脆弱性（CAN-2005-0555）
   上記のInternet Explorerに関する脆弱性を攻撃者が悪用するには、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。
6. 本件は、Exchange Serverに関する脆弱性です。
   SVPはサブシステム管理専用装置であり、Exchange Serverがインストール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。
7. 本件は、MSN Messengerに関する脆弱性です。
   SVPはサブシステム管理専用装置であり、MSN Messengerがインストール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。

8. 本件は、Microsoft Wordに関する脆弱性です。
   SVPはサブシステム管理専用装置であり、Microsoft Wordがインストール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。

弊社ストレージ装置における、今回の脆弱性の影響を以下の表に示します。

表1 脆弱性の影響範囲

ストレージ装置	影響する脆弱性
Hitachi Universal Storage Platform Hitachi Universal Storage Platform H12000	MS05-019
SANRISE9900Vシリーズ SANRISE H1024/128	MS05-019

現在までのところ、SVPに影響があるMS05-019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

攻撃者が、MS05-019の脆弱性を悪用し、特別な細工を施したTCPメッセージやICMPメッセージを対象となるコンピュータに送信することにより、リモートでコードが実行される可能性、TCP接続をリセットされる可能性、リクエスト応答が停止される可能性があります。

3. 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。

4. 対策の内容

マイクロソフト社より提供されている対策パッチの適用を、弊社保守員が実施させていただきます。現在、本件に関する対策準備を進めております。20日ほどで対策準備が整う予定でございます。対策準備が整い次第、弊社保守員よりご連絡申し上げます。本パッチの適用により、今回問題となっている脆弱性は対策されます。

5. Worm/Virusに対するSANRISEの見解

今回のように、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、対策を実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。

6. Storage Navigatorのご使用について

Storage Navigatorを使用されている場合、クライアントPCのOSによっては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/ms05-016.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-017.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-018.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-019.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-020.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-021.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-022.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-023.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