セキュリティ情報（2005年2月10日）

SANRISEシリーズにおけるSVPセキュリティホール（MS05-004～015）対策について

2005年2月10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. MS05-004：ASP.NETパス検証の脆弱性（887219）
2. MS05-005：Microsoft Office XPの脆弱性により、リモートでコードが実行される（873352）
3. MS05-006：Windows SharePoint ServicesおよびSharePoint Team Servicesの脆弱性により、クロスサイトスクリプティングおよびなりすましの攻撃が行なわれる（887981）
4. MS05-007：Windowsの脆弱性により、情報漏えいが起こる（888302）
5. MS05-008：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（890047）
6. MS05-009：PNG処理の脆弱性により、リモートでコードが実行される（890261）
7. MS05-010：ライセンスログサービスの脆弱性により、コードが実行される（885834）
8. MS05-011：サーバメッセージブロックの脆弱性により、リモートでコードが実行される（885250）
9. MS05-012：OLEおよびCOMの脆弱性により、リモートでコードが実行される（873333）
10. MS05-013：DHTML編集コンポーネントのActive Xコントロールの脆弱性により、リモートでコードが実行される（891781）
11. MS05-014：Internet Explorer用の累積的なセキュリティ更新プログラム（867282）
12. MS05-015：ハイパーリンクオブジェクトライブラリの脆弱性により、リモートでコードが実行される（888113）

弊社のSANRISEシリーズのSVPにおける、上記1～12の脆弱性の影響は下記の通りです。

1. 本件は、ASP.NETに関する脆弱性により、Webサイトのセキュリティ設定が無視され、不正アクセスが行なわれる可能性があるというものです。
   SVPはサブシステム管理専用装置であり、ASP.NETを使用したWebアプリケーションが動作す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、Microsoft Office XP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 Office XP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。
3. 本件は、Windows SharePoint Services for Windows Server 2003およびSharePoint Team Services from Microsoft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、これらのソフトウェア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。
4. 本件は、Windowsの名前付きパイプに関する脆弱性であり、対象となるOSはWindows XP です。
   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を使用しているため、本脆弱性の影響を受けます。
5. 本件は、Windowsのドラッグアンドドロップ処理に関する脆弱性により、権限の昇格が行わ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、Windows Media Player、Windows Messenger、MSN MessengerにおけるPNGの処理に関する脆弱性により、リモートでコードが実行されるというものです。
   SVPはサブシステム管理専用装置であり、これらのソフトウェアの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。
7. 本件は、ライセンスログサービスに関する脆弱性であり、対象となるOSはWindows NT Server 4.0、Windows 2000 Server、Windows Server 2003です。
   SVPではこれらのOSを使用していませんので、本脆弱性の影響は受けません。
8. 本件は、Windowsのサーバメッセージブロックに関する脆弱性であり、対象となるOSはWindows 2000、Windows XP、Windows Server 2003です。
   弊社のSANRISE9980V/9970V、SANRISE9980V-e/9970V-eおよびSANRISE H1024/ H128では、SVPのOSとしてWindows 2000を使用しているため、本脆弱性の影響を受けます。また、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を使用しているため、本脆弱性の影響を受けます。
9. MS05-012に含まれる脆弱性と影響は下記の通りです。

a. COM構造化ストレージの脆弱性（CAN-2005-0047）
本件は、COM構造化ストレージの脆弱性により、権限の昇格が行なわ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、コンピュータにログオンして特別な細工が施されたプログラムを実行するように、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。

b. 入力の検証の脆弱性（CAN-2005-0044）
本件は、OLEに関するバッファオーバーフローの脆弱性により、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OLEオブジェクトを含む電子メールメッセージを開くように、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。

10. 本件は、DHTML編集コンポーネントのActive Xコントロールに関するクロスドメインの脆弱性により、情報の漏えいまたは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。

11. MS05-014に含まれる脆弱性と影響は下記の通りです。
a. ドラッグアンドドロップの脆弱性（CAN-2005-0053）
b. URLのデコーディングゾーンのなりすましの脆弱性（CAN-2005-0054）
c. DHTMLメソッドのヒープメモリの破壊の脆弱性（CAN-2005-0055）
d. チャンネル定義形式（CDF）のクロスドメインの脆弱性（CAN-2005-0056）
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。

12. 本件は、ハイパーリンクオブジェクトに関するバッファオーバーフローの脆弱性により、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リンクを作成し、Webサイトまたは電子メールメッセージ上の悪質なハイパーリンクを選択するように、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。

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	MS05-007 MS05-011
SANRISE9900Vシリーズ SANRISE H1024/128	MS05-011

現在までのところ、SVPに影響があるMS05-007およびMS05-011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

1. MS05-007
攻撃者が綿密な細工を施したリクエストを対象となるコンピュータに送信することにより、共有リソースにアクセスしたユーザのユーザ名をリモートで読み取られる可能性があります。この脆弱性により、攻撃者はリモートでコードを実行したり、権限を昇格させることはできませんが、攻撃に使用する情報を得ることが可能です。

2. MS05-011
攻撃者が特別な細工を施したメッセージを作成し、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があります。この脆弱性を悪用することで、攻撃者は影響を受けるコンピュータをリモートで完全に制御す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。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/ms05-004.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-005.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-006.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-007.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-008.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-009.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-010.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-011.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-012.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-013.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-014.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms05-015.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