セキュリティ情報（2004年10月15日）

SANRISEシリーズにおけるSVPセキュリティホール（MS04-029～038）対策について

2004年10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. MS04-029：RPCランタイムライブラリの脆弱性により、情報漏えいおよびサービス拒否が起こる（873350）
2. MS04-030：WebDAV XML Messageハンドラの脆弱性によりサービス拒否が起こる（824151）
3. MS04-031：NetDDEの脆弱性により、リモートでコードが実行される（841533）
4. MS04-032：Microsoft Windowsのセキュリティ更新プログラム（840987）
5. MS04-033：Microsoft Excelの脆弱性により、コードが実行される（886836）
6. MS04-034：圧縮（zip形式）フォルダの脆弱性により、コードが実行される（873376）
7. MS04-035：SMTPの脆弱性により、リモートでコードが実行される（885881）
8. MS04-036：NNTPの脆弱性により、コードが実行される（883935）
9. MS04-037：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（841356）
10. MS04-038：Internet Explorer用の累積的なセキュリティ更新プログラム（834707）

弊社のSANRISEシリーズのSVPにおける、上記1～10の脆弱性の影響は下記の通りです。

1. 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。
2. 本脆弱性は、対象となるコンピュータ上のIISサーバでWebDAVサービスを起動している場合に影響を受けます。
   弊社のSANRISEシリーズのSVPはサブシステム管理専用装置であり、本サービス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。
3. 本脆弱性は、対象となるコンピュータ上でNetDDEサービスを起動している場合に影響を受けます。
   弊社のSANRISEシリーズのSVPはサブシステム管理専用装置であり、本サービス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。
4. MS04-032に含まれる脆弱性と影響は下記の通りです。
   a. 「Windows Management」の脆弱性（CAN-2004-0207）
      本件は、Windows Management API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。
   b. VDM（仮想DOSマシン）の脆弱性（CAN-2004-0208）
      本件は、VDM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。
   c. Graphics Rendering Engineの脆弱性（CAN-2004-0209）
      本件は、Graphics Rendering Engine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画像ファイルを作成し、この細工されたファイルをExplorerやIE等で開くように、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。
   d. Windowsカーネルの脆弱性（CAN-2004-0211）
      Windows 2000およびWindows XPでは、本脆弱性の影響を受けません。このため、SVPでは本脆弱性の影響は受けません。
5. 本脆弱性の対象は、Microsoft Excelです。
   SVPでは本脆弱性の影響は受けません。
6. 本脆弱性の対象OSはWindows XPまたはWindows Server 2003となっています。
   SANRISE9900Vシリーズおよび SANRISE H1024/128では、OSがWindows2000であるため影響を受けません。また、Hitachi Universal Storage PlatformおよびHitachi Universal Storage Platform H12000ではOSがWindows XPのため対象となりますが、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zip形式のファイルを作成し、この細工されたファイルをExplorerやIE等で開くように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。

7. 本脆弱性の対象OSはWindows XP 64-Bit EditionまたはWindows Server 2003となっています。
   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。
8. 本脆弱性の対象OSはWindows NT Server 4.0、Windows 2000 Server、Windows Server 2003となっています。
   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。
9. MS04-037に含まれる脆弱性と影響は下記の通りです。
   a. シェルの脆弱性（CAN-2004-0214）
      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、IEを使用した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. Program Group Converterの脆弱性（CAN-2004-0572）
      本件は、Program Group Converter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、IEを使用した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. MS04-038には以下の脆弱性が含まれています。
    a. CSSヒープメモリの破損の脆弱性（CAN-2004-0842）
    b. 類似したメソッド名によるリダイレクトのクロスドメインの脆弱性（CAN-2004-0727）
    c. インストールエンジンの脆弱性（CAN-2004-0216）
    d. ドラッグアンドドロップの脆弱性（CAN-2004-0839）
    e. 2バイト文字セットを使用するシステムにおけるアドレスバーのなりすましの脆弱性（CAN-2004-0844）
    f. プラグインナビゲーションアドレスバーに使用したなりすましの脆弱性（CAN-2004-0843）
    g. 画像タグのスクリプトによるファイルダウンロードの脆弱性（CAN-2004-0841）
    h. SSLキャッシュの脆弱性（CAN-2004-0845）
    上記のIEの脆弱性を攻撃者が悪用するには、対象となるPC上でWebページを表示したり電子メールを表示している事、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）を誘導する事、等が必要条件となります。SVPはサブシステム管理専用装置であり、IEを使用した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。

上記のことから、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/ms04-029.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-030.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-031.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-032.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-033.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-034.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-035.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-036.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-037.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-038.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