セキュリティ情報（2004年7月16日）

SANRISE9900V/9900V-e、H1024/128におけるSVPセキュリティホール（MS04-018～024）対策について

2004年7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. MS04-018：Outlook Express用の累積的なセキュリティ更新プログラム（823353）
2. MS04-019：ユーティリティマネージャの脆弱性により、コードが実行される（842526）
3. MS04-020：POSIXの脆弱性により、コードが実行される（841872）
4. MS04-021：Internet Information Server 4.0のセキュリティ更新プログラム（841373）
5. MS04-022：タスクスケジューラの脆弱性により、コードが実行される（841873）
6. MS04-023：HTMLヘルプの脆弱性により、コードが実行される（840315）
7. MS04-024：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（839645）

弊社のSANRISE9900Vシリーズにおける、上記1～7の脆弱性の影響は下記の通りです。

1. この脆弱性の対象は、Outlook Expressです。
   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を搭載していますが、SVPはサブシステム管理専用装置であるため、Outlook Expressが実行されることはありません。よって、本脆弱性の影響は受けません。
2. この脆弱性を悪用するには、対象となるPCでユーティリティマネージャを起動し、特別な細工を施したメッセージをユーティリティマネージャに送信するプログラムを実行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。よって、本脆弱性の影響は受けません。
3. この脆弱性はPOSIX（Portable Operating System Interface for UNIX）に関するものです。
   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。よって、本脆弱性の影響は受けません。
4. この脆弱性の対象となるOSはWindows NT 4.0のみです。
   SVPのOSはWindows2000であるため、本脆弱性の影響は受けません。
5. この脆弱性を悪用するには、タスクスケジューラで使用する .jobファイルに特別な細工を施し、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。よって、本脆弱性の影響は受けません。
6. 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、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。よって、本脆弱性の影響は受けません。
7. 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、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。よって、本脆弱性の影響は受けません。

よって、上記7件の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

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. Remote Console Storage Navigatorのご使用について

Remote Console Storage Navigatorのご使用については、Remote Console 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/ms04-018.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-019.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-020.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-021.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-022.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-023.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms04-024.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