セキュリティ情報（2009年8月19日）

日立ディスクアレイサブシステムにおけるSVPセキュリティホール（MS09-034～044）対策について

2009年8月19日
（株）日立製作所RAIDシステム事業部

1. 日立ディスクアレイサブシステム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. MS09-034：Internet Explorer用の累積的なセキュリティ更新プログラム（972260）
2. MS09-035：Visual StudioのActive Template Libraryの脆弱性により、リモートでコードが実行される（969706）
3. MS09-036：Microsoft WindowsのASP.NETの脆弱性により、サービス拒否が起こる（970957）
4. MS09-037：Microsoft ATL (Active Template Library) の脆弱性により、リモートでコードが実行される（973908）
5. MS09-038：Windows Mediaファイル処理における脆弱性により、リモートでコードが実行される（971557）
6. MS09-039：WINSの脆弱性により、リモートでコードが実行される（969883）
7. MS09-040：メッセージキューの脆弱性により、特権が昇格される（971032）
8. MS09-041：ワークステーションサービスの脆弱性により、特権が昇格される（971657）
9. MS09-042：Telnetの脆弱性により、リモートでコードが実行される（960859）
10. MS09-043：Microsoft Office Web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（957638）
11. MS09-044：リモートデスクトップ接続の脆弱性により、リモートでコードが実行される（970927）

弊社の日立ディスクアレイサブシステムのSVPにおける、上記1～11の脆弱性の影響は下記の通りです。

1. 本件は、Internet Explorer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。
本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。
2. 本件は、Visual StudioのActive Template Library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はサブシステム管理専用装置でありVisual Studioがインストールされることはありません。また、Visual C++再頒布可能パッケージもインストールされません。このため、SVPでは本脆弱性の影響は受けません。
3. 本件は、Microsoft WindowsのASP.NETの脆弱性により、サービス拒否が起こるというものです。
SVPでは、本件の対象となるOSを使用していないため、本脆弱性の影響は受けません。
4. 本件は、Microsoft ATL (Active Template Library) 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。
本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。
5. 本件は、Windows Mediaファイル処理における脆弱性により、リモートでコードが実行されるというものです。
本脆弱性を攻撃者が悪用するには、特別に細工された AVIファイル、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、WINS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では、本件の対象となるOSを使用していないため、本脆弱性の影響は受けません。
7. 本件は、メッセージ キューの脆弱性により、特権が昇格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、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、ワークステーション サービスの脆弱性により、特権が昇格されるというものです。
日立ディスクアレイサブシステムのSVPでは、本件の対象となるOSを使用しており、本脆弱性の影響を受けます。
9. 本件は、Telnet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。
本脆弱性を攻撃者が悪用するには、特別に細工された Telnetサーバーにアクセスするように、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。
10. 本件は、Microsoft Office Web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はサブシステム管理専用装置であり、Microsoft Office Web コンポーネント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。

11. 本件は、リモートデスクトップ接続の脆弱性により、リモートでコードが実行されるというものです。
本脆弱性を攻撃者が悪用するには、特別に細工された RDP サーバーにアクセスさせる、または、特別な細工が施されたWebペ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。

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 V Hitachi Universal Storage Platform H24000 Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H20000	MS09-041
Hitachi Universal Storage Platform Hitachi Universal Storage Platform H12000 Hitachi Network Storage Controller Hitachi Universal Storage Platform H10000	MS09-041
SANRISE9900Vシリーズ SANRISE H1024/128	なし

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。また日立ディスクアレイサブシステム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、上記の脆弱性を悪用する目的で、特別な細工を施したRPCメッセージを作成し、影響を受け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。

3. 対象製品

Hitachi Universal Storage Platform V、Hitachi Universal Storage Platform H24000、
Hitachi Universal Storage Platform VM、Hitachi Universal Storage Platform H20000、
Hitachi Universal Storage Platform、Hitachi Universal Storage Platform H12000、
Hitachi Network Storage Controller、Hitachi Universal Storage Platform H10000、
SANRISE9980V/9970V、SANRISE9980V-e/9970V-e、SANRISE H1024/ H128

注 :Hitachi Adaptable Modular Storage、Hitachi Workgroup Modular Storage、Hitachi Simple Modular Storage、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. 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/ms09-034.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-035.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-036.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-037.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-038.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-039.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-040.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-041.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-042.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-043.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms09-044.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