セキュリティ情報（2010年9月17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（MS10-061～069）対策について

2010年9月17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. MS10-061：印刷スプーラーサービスの脆弱性により、リモートでコードが実行される（2347290）
2. MS10-062：MPEG-4コーデックの脆弱性により、リモートでコードが実行される（975558）
3. MS10-063：Unicodeスクリプトプロセッサの脆弱性により、リモートでコードが実行される（2320113）
4. MS10-064：Microsoft Outlookの脆弱性により、リモートでコードが実行される（2315011）
5. MS10-065：Microsoftインターネットインフォメーションサービス（IIS）の脆弱性により、リモートでコードが実行される（2267960）
6. MS10-066：リモートプロシージャーコールの脆弱性により、リモートでコードが実行される（982802）
7. MS10-067：ワードパッドのテキストコンバーターの脆弱性により、リモートでコードが実行される（2259922）
8. MS10-068：Local Security Authority Subsystem Service（LSASS）の脆弱性により、特権が昇格される（983539）
9. MS10-069：Windowsクライアント/サーバーランタイムサブシステムの脆弱性により、特権が昇格される（2121546）

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1～9の脆弱性の影響は下記の通りです。

1. 本件は、印刷スプーラーサービスの脆弱性により、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、攻撃者が共有された印刷スプーラーに特別に細工した印刷リクエストを送信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り、印刷スプーラーを共有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、MPEG-4コーデックの脆弱性により、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利用するには、特別に細工されたファイルを開くように、SVP使用者（保守員）を誘導する必要があります。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。
3. 本件は、Unicodeスクリプトプロセッサの脆弱性により、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利用するには、特別に細工されたファイルを開くように、SVP使用者（保守員）を誘導する必要があります。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、Microsoft Outlook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 Outlook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。
5. 本件は、Microsoftインターネットインフォメーション サービス（IIS）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利用するためには、クライアントから特別に細工されたHTTPリクエストをSVPに送信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り、IISがHTTPリクエストを受信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。
6. 本件は、リモートプロシージャーコールの脆弱性により、リモートでコードが実行されるというものです。
本脆弱性を攻撃者が利用するには、SVP使用者（保守員）に悪意のあるサーバーへのRPC接続を開始させる必要があります。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. 本件は、ワードパッドのテキストコンバーターの脆弱性により、リモートでコードが実行されるというものです。
本脆弱性を攻撃者が利用するには、特別に細工されたファイルを開くように、SVP使用者（保守員）を誘導する必要があります。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。

8. 本件は、Local Security Authority Subsystem Service（LSASS）の脆弱性により、特権が昇格されるというものです。
   本脆弱性により攻撃を受けるのは、Active Directory、Active Directory Application Mode（ADAM）およびActive Directory Lightweight Directory Service（AD LDS）が稼動している必要があります。SVPはサブシステム管理専用装置であり、このようなモジュール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。
9. 本件は、Windowsクライアント/サーバーランタイムサブシステムの脆弱性により、特権が昇格されるというものです。
   本脆弱性を攻撃者が利用するためには、SVPにログオン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り、SVP使用者（保守員）によ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。

よって、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 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。

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/ms10-061.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-062.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-063.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-064.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-065.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-066.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-067.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-068.mspx
http://www.microsoft.com/japan/technet/security/bulletin/ms10-069.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

ページの先頭へ