セキュリティ情報（2004年1月16日）

SANRISE9900V/9900V-e、H1024/128におけるSVPセキュリティホール（MS04-003）対策について

2004年1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

Windows2000/XP、Windows Server 2003およびSQL Server 2000に対して、下記に示す新たなセキュリティホールが発見されました。

1. MS04-003：MDAC機能のバッファオーバランにより、コードが実行される（832483）

今回のセキュリティホールは、WindowsおよびSQL Serverに同梱されているMDAC（Microsoft Data Access Components）に関するものです。MDACはリモートデータベースへの接続等、データベースの基本オペレーションで使用されます。本脆弱性を悪用することにより、攻撃者は対象となるコンピュータに対しバッファオーバフローを起こさせ、任意のコードを実行させる可能性があります。

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を搭載しており、外部からの管理のためLANに接続することが可能となっております。
しかし今回のセキュリティホールでは、攻撃者が攻撃を行なうには、標的とするコンピュータと同じIPサブネット上でSQL Serverをシミュレートすることが必要条件となっており、対象となるコンピュータがネットワーク上のSQL Serverを探すために送信したブロードキャスト・リクエストに対して細工をしたパケットで応答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、上記ブロードキャスト・リクエストを送信するSQL管理ツールがインストールされることはありません。
そのため、今回の脆弱性の影響を受けることはなく、特に対策は必要ありません。

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、クライアントPCがWindows2000/XPまたはWindows Server 2003であっても、Remote Console Storage Navigator機能に限ったご使用であれば問題ありません。
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/ms04-003.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