セキュリティ情報（2004年3月15日）

SANRISE9900V/9900V-e、H1024/128におけるW32.Blaster.Worm等の対策について

2004年3月15日
（株）日立製作所RAIDシステム事業部

1. SANRISE9900Vに対するW32.Blaster.Worm対策のお願い

既にニュース等で御存知の通り、Windows2000/XP/NT を対象といたしましたWormプログラム、W32.Blaster.Wormおよびその亜種が現在全世界的に蔓延しております。
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。
万一、本Wormに感染しますとSVPが再起動を繰り返すという現象になる危険がございます。
SVPは直接ストレージ機能には係わりませんので、万一感染いたしましてもストレージとしてのデータの内容およびRead/Write機能には支障はございません。
しかしながら装置の遠隔監視が妨げられたり、設定変更が行いにくくなる等の可能性があります。またLANを経由して他のPCに対して感染を広める危険性もございます。
そのため今般、対象となる製品に対しまして、感染の有無の確認および予防処置をさせていただき、万一感染していた場合はその対策をとらせていただきます。
御迷惑をおかけいたしますが、何卒よろしくお願い申し上げます。

2. W32.Blaster.Wormの特徴

従来の多くのWorm、Virusはメールの受信・開封やWeb Siteへのアクセスにより感染を広めるものでした。
SANRISE9900VのSVPは装置管理専用装置として運用されるため、メールの受信やWeb Siteへのアクセス等は行なわれず、それらの危険性はありませんでした。
しかしながら今回のW32.Blaster.Wormおよびその亜種は、Windows2000のRPC機能を利用して外部より送りつけられます。そのため感染したPCと同じネットワークに接続しているだけで感染する特徴がございます。したがってSVPがLANに接続されている場合は感染する危険性がございます。

3. 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。

4. 発生条件

SVPが装置外部のLANに接続され、そのLANを介したネットワーク上に感染したPCが接続された場合。（ただし、Firewall等の設定によっては防御できる場合もございます）
具体的には、例えばOpenView、JP1/HiCommand等のシステム管理ソフトにより装置外部のサーバを用いてサブシステムの管理を行なっている場合、危険性がございます。

5. 対策の内容

次の対策作業を、弊社保守員が実施させていただきます。
感染の有無を確認した上で、未感染であればマイクロソフト社より提供されている対策パッチ（Windows2000-KB823980-x86-ENU他）を搭載します。本パッチにより今回問題となっている脆弱性はカバーされます。
万一感染していた場合は、その状況に応じて駆除もしくは感染SVPの交換を行ないます。

6. Worm/ Virusに対するSANRISEの見解

今回のようにネットワーク接続だけで感染する等、通常のSANRISEの運用でも感染する危険性が生じた場合には、逐次その旨お知らせすると共に、対策を施させていただきます。
情報の提供はご覧のWebへ掲載する他、サポート契約に基づく「Software Support News」にてお知らせいたします。

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

Storage Navigator を使用されている場合、クライアントPCがWindows2000/XP/NTであれば同様の対策が必要と思われます。
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/

更新履歴

2004年3月15日　対策パッチ名称　誤記訂正
2003年8月20日　新規情報掲載

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