Nortel Threat Protection System SEU/Rule Update 02/15/2006

Date: 02/15/2006

This rules update is Snort Engine Update (SEU) #14 for the 4.1 series and Rule Pack 44 for the 3.2 series of the Nortel Threat Protection System Defense Center and Intrusion Sensor. This rules update applies to the TPS 2070 Defense Center and all TPS 2x50/2x70 Intrusion Sensor models.

Software Files and File Names:

TPS 4.1 Series SEU#14	**TPS_Snort_Engine_Upgrade-14-vrt-sh**
TPS 3.2 Series Rule Pack#44	**Nortel_TPSRule_Pack-3.2.0-44.sh**

02/15/2006 Rule Update Synopsis:

The Nortel Threat Protection System Team has learned of multiple vulnerabilities affecting hosts using the Microsoft operating system. The TPS team has also added rules to detect Skype usage as well as attacks aimed at Qualcomm Worldmail and other applications.

Details:

Microsoft Security Bulletin MS06-005 -Microsoft Media Player plugin is subject to a buffer overflow condition when handling embedded media in web pages. The plugin is used in Mozilla browsers on hosts using the Microsoft Windows operating system.

A value of more than 2081 bytes in the src tag of an embedded component handled by Windows media player may present an attacker with the opportunity to overflow a fixed length buffer and execute code of their choosing on a vulnerable host. A rule to detect attacks targeting this vulnerability is included in this update and is identified as sid 5710.

Microsoft Security Bulletin MS06-006 - Windows Media Player suffers from a programming error that may enable an attacker to run code of their choosing on a vulnerable system. The error occurs when processing malformed bitmap files with the application. A bitmap file with length zero is not correctly checked for actual length, and it may be possible for an attacker to create a malicious image with size 0 but with actual data in the image that can be copied into memory for execution. A rule to detect attacks targeting this vulnerability is included in this update and is identified as sid 5711.

WARNING:

Nortel Threat Protection System customers must upgrade to 4.1.0.1 prior to applying SEU #14. Nortel Threat Protection System customers must upgrade to 3.2.0.3 or higher in order to utilize the enhanced rules in Rule Pack 44. Failure to apply these patches will result in sensor failure when installing these rules.

Snort Engine Updates:

In Threat Protection System v4.1, Snort Engine Updates (SEUs) replace rule pack updates as the mechanism for updating Snort and Snort-based rules. In addition, SEUs can provide new and updated preprocessors and protocol decoders that aid in detecting intrusion attempts.

Note that SEUs can contain new binaries (in the form of shared object rules and new versions of Snort), so make sure that your process for installing new SEUs complies with your network and security policies.

Shared Object Rules

Shared object rules (SORs) are a new type of rule that allows the Nortel Threat Protection System Team more flexibility in detecting possible intrusions. SORs are delivered in SEUs in binary format as compared with the text rules (now called standard text rules or STRs) that were provided in previous rule packs.

You can view the rule documentation and create copies of shared object rules just as you could with standard text rules. However, you can only view and modify attributes such as the message or the source and destination ports and addresses in the rule header. You cannot view or modify the rule keywords section, including rule content keywords. Note that you can still create and modify your own standard text rules, and you can view, copy, and modify any of the legacy standard text rules.

How to get help:

If you have purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4 NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to http://www.nortel.com/support . Click on the link for Express Routing Codes located at the bottom-right corner of the Web page.