Nortel Threat Protection System SEU/Rule Update 04/26/2006

Date: 04/26/2006

This rules update is Snort Engine Update (SEU) #24 for the 4.1 series and Rule Pack 49 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#24	**TPS_Snort_Engine_Upgrade-24-vrt-sh**
TPS 3.2 Series Rule Pack#49	**Nortel_TPSRule_Pack-3.2.0-49.sh**

04/26/2006 Rule Update Synopsis:

The Nortel Threat Protection System Team has added multiple rules to detect the use of Spyware and potentially unwanted technology on a protected network. These rules have been given their own category and a new rule group. The TPS team has also modified and improved numerous other rules.

Details:

Spyware-put.rules - This new rule category contains rules to detect the use of numerous spyware and other potentially unwanted technology using Snort. More than 250 new rules have been added to this group.

Note:
The spyware-put.rules category only applies to version 4.1.x. These rules are not available for earlier models of the Intrusion Sensor.

Backdoor.rules - The backdoor.rules group has been modified and updated to better detect the use of trojan horse programs on a protected network. More than 150 new rules have been added to detect new trojan horse programs and variations on older remote administration tools. Each rule is also accompanied by detailed documentation for each spyware, trojan and potentially unwanted software to assist in determining the likelihood of infection and has relevant links to information regarding their removal.

WARNING:

Nortel Threat Protection System customers must upgrade to 4.1.0.2 prior to applying SEU #24. Nortel Threat Protection System customers must upgrade to

3.2.0.3 or higher in order to utilize the enhanced rules in Rule Pack 49. 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.