Nortel Threat Protection System SEU/Rule Update

Date: 02/19/2007

Software Files and File Names:

TPS 4.5.1 Series SEU#64	**TPS_Snort_Engine_Upgrade-64-vrt.sh**
TPS 4.6 Series SEU #64	**TPS_Snort_Engine_Upgrade-64-vrt.sh**

Rule Update Synopsis:

Nortel has learned of a remotely exploitable vulnerability in the DCE/RPC preprocessor. This preprocessor is vulnerable to a stack-based buffer overflow that could potentially allow attackers to execute code with the same privileges as the Snort binary. This vulnerability has been identified as CVE-2006-5276.

IMPORTANT! The DCE/RPC preprocessor is enabled by default in the predefined intrusion policies on version 4.6.x Intrusion Sensors and Defense Centers. It is disabled by default in version 4.5.x Intrusion Sensors and Defense Centers.

Details:

|| New Features and Functionality

SEU 64 includes an updated DCE/RPC preprocessor.

|| Issues Resolved in SEU 64

The following issues are resolved in SEU 64:

- Resolved an issue with the DCE/RPC preprocessor (33525).

|| Importing the SEU

This SEUs can contain new binaries. Make sure your process for uploading and installing SEUs complies with your security policies.

If your Nortel TPS deployment includes two Defense Centers configured as a high availability pair, you only need to import and apply the SEU on one of the Defense Centers. The second Defense Center receives the SEU as part of the regular synchronization process.

WARNING! This SEU does not support version 4.1.x or earlier. If your Intrusion Sensor has not been upgraded to version 4.5.x or later and you manually enabled the DCE/RPC preprocessor through a setting in the `user.conf` file, you must either disable the preprocessor in the `user.conf` file or upgrade

your sensor to the latest version and import this SEU. See Updating the user.conf File in v4.1.x for more information.

Installation Instructions for Versions 4.5.x and 4.6.x

Manually Importing SEUs

The following procedure explains how to import a new SEU onto a Defense Center or Intrusion Sensor that does not have direct access to the Internet.

TIP! If you use a Defense Center to manage your Intrusion Sensors, you can download and import the SEU to the Defense Center. When you apply an intrusion policy to a managed Intrusion Sensor, the appropriate parts of the SEU are automatically pushed to the sensor.

To update an SEU manually:

1. From a computer that can access the Internet, access and log into Nortel Support (https://support.nortel.com/).
2. Navigate to the SEU for your appliances and save it to your computer.
3. Log into the web interface for your Intrusion Sensor or Defense Center.
4. Select **Policy & Response > Intrusion Sensor > Rules** .

   The Rules page appears.
5. Click **Import Rules** .

   The Import Rules page appears.
6. Select **SEU or text rule file to upload and apply** and click **Browse** to navigate to and select the SEU file.
7. For any new rules in the SEU, Nortel sets a default rule state, either enabled or disabled. For example, if the vulnerability that the rule detects is relatively innocuous and unlikely to affect many networks, the VRT may set the rule state to Disabled. However, if the rule detects a widespread vulnerability that has a known exploit, the VRT may set the rule state to Enabled.

   Specify how you want to set the rule state for new rules after import:

   - If you want any new rules to use the default rule state set by Nortel in your existing policies, select **In the default state**.
   - If you want to disable new rules, select **In the disabled state.**

   TIP! If you import an SEU using the **In the default state** option, any old or deprecated rules that the VRT marked for deletion in the SEU are automatically disabled and then moved to the `deleted.rules` file. You can enable these rules under the Deleted Rules category on the Rule State page as part of a custom intrusion policy. You can also copy a deleted rule and use it as the basis for a custom intrusion rule.
8. Click **Update**.

The rules are updated. However, the rules are not activated until the next time you build and apply the affected intrusion policies.

IMPORTANT! Intrusion Sensors do **not** use the new rule set for inspection until after you re-apply your intrusion policies. See "Applying an Intrusion Policy" in your user guide for more information.

WARNING: Nortel Threat Protection System customers must upgrade to 4.5.1 prior to applying this patch. Failure to upgrade will result in sensor failure when installing these rules.

Snort Engine Updates: In Threat Protection System v4.1, Snort Engine Updates (SEUs) replaced 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, and 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.