**Nortel Threat Protection System SEU/Rule Update**

Date: 05/14/2007

Software Files and File Names:

| | |
|---|---|
| TPS 4.5.1 Series SEU#76 | **TPS_Snort_Engine_Upgrade-76-vrt.sh** |
| TPS 4.6 Series SEU #76 | **TPS_Snort_Engine_Upgrade-76-vrt.sh** |

This update is SEU 76 for all models of the 4.6 and 4.5 series of the Defense Center and Intrusion Sensor.

# Synopsis:

The Nortel TPS team is aware of a vulnerability affecting an ActiveX control used by Symantec Norton AntiVirus products.

This release also contains an updated detection engine.

# Details:

This release contains an updated detection engine with enhanced HTTP POST normalization. This release also contains:

- A new http_post rule keyword used to search for content in normalized HTTP posts
- A fix for a potential memory leak when generating HTTP Inspection events

**NOTE:** In the default configuration, the http_inspect preprocessor will generate informational events on normalized HTTP POST data. To disable these events refer to the User Guide.

**Symantec Norton AntiVirus ActiveX Control (CVE-2006-3456):**
An ActiveX control used by Symantec Norton AntiVirus products contains a vulnerability that may allow an attacker to execute code on an affected host.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 11268 through 11271.

**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.