Nortel Threat Protection System SEU/Rule Update

Date: 11/30/2006

Software Files and File Names:

TPS 4.1 Series SEU#52	**TPS_Snort_Engine_Upgrade-52-vrt.sh**
TPS 4.5.1 Series SEU#52	**TPS_Snort_Engine_Upgrade-52-vrt.sh**

Rule Update Synopsis:

This SEU contains an updated detection engine. There are no new or modified rules in this SEU.

Details:

This SEU contains an improved version of the Intrusion Sensor detection engine with performance enhancements, and also resolves the following issues:

- Fixed SMB fragmentation handling in the DCE/RPC preprocessor.
- Fixed session handling so that Snort continues to process packets if TCP sequence numbers wrap in a TCP session.

WARNING: Nortel Threat Protection System customers must upgrade to 4.1.0.2 or 4.5.1 (as applicable) 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) 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