Nortel Threat Protection System SEU/Rule Update

Date: 03/08/2007

Software Files and File Names:

TPS 4.5.1 Series SEU#67	**TPS_Snort_Engine_Upgrade-67-vrt.sh**
TPS 4.6 Series SEU #67	**TPS_Snort_Engine_Upgrade-67-vrt.sh**

Rule Update Synopsis:
This update is SEU 67 for all models of the 4.6 and 4.5 series of the Defense Center and Intrusion Sensor.

The SEU is aware of vulnerabilities affecting HP Mercury Loadrunner, Shockwave, Trend Micro Officescan and Wordpress. This release also includes more additions to the spyware-put and backdoor rule sets.

Details:

HP Mercury LoadRunner CVE-2007-0446:
The HP Mercury LoadRunner agent suffers from a programming error that may allow a remote attacker to cause a stack-based buffer overflow condition to occur. This may lead to code execution of the attacker's choosing.
A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 10187.

Trend Micro OfficeScan CVE-2007-0325:
The Trend Micro OfficeScan Web-Deployment ActiveX control contains a programming error that may allow remote attackers to execute code on an affected host via a specially crafted web page.
Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 10173 through 10175.

WordPress CVE-2007-1277:
The WordPress 2.1.1 source code was compromised by an attacker who then introduced a backdoor into the application. This may allow other attackers to execute commands or code of their choosing on an affected server.
Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 10196 and 10197.

Macromedia Shockwave Flash ActiveX control:
Macromedia Shockwave Flash contains a programming error that may allow a remote attacker to execute code of their choosing on an affected host using the ActiveX control.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 10214 through 10216.

Also, the SEU has added multiple new rules to the backdoor and spyware-put categories in this release.

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.

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.