Nortel Threat Protection System SEU/Rule Update

Date: 12/132006

Software Files and File Names:

TPS 4.1 Series SEU#54	**TPS_Snort_Engine_Upgrade-54-vrt.sh**
TPS 4.5.1 Series SEU#54	**TPS_Snort_Engine_Upgrade-54-vrt.sh**

Rule Update Synopsis:

The VRT is aware of vulnerabilities affecting the Microsoft Operating System and has introduced new rules to provide coverage for exploitation attempts targeting these vulnerabilities.

Details:

Microsoft Security Bulletin MS06-078:
A vulnerability in the way that Microsoft Windows Media Player handles Advanced System Format (ASF) files may allow a remote attacker to execute code of their choosing on an affected system.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9625.

Microsoft Security Bulletin MS06-077:
The Microsoft Remote Install Service suffers from a programming error that may allow an attacker to upload files of their choosing onto the TFTP server that may then be installed onto machines using the service.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9638.

Microsoft Security Bulletin MS06-076:
Microsoft Outlook Express does not correctly handle malformed Windows Address Book files. A remote attacker may be able to execute code of their choosing by supplying a specially crafted address book file to be read on a vulnerable host.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9639.

Rules that may also indicate attacks targeting this vulnerability were previously released and are identified as SIDs 6412 and 6413.

Microsoft Security Bulletin MS06-074:
A vulnerability in the Microsoft SNMP service may allow a remote attacker to execute code of their choosing on a vulnerable system by supplying a malformed SNMP request to the service.

Rules to detect attacks targeting this vulnerable service were previously released and are identified as SIDs 1411 through 1414.

Microsoft Security Bulletin MS06-073:
Microsoft Visual Studio uses a WMI Wizard that does not correctly handle malformed WMI objects. This may allow a remote attacker to execute code of their choosing on a vulnerable host via a specially crafted web page.

Rules to detect attacks targeting this vulnerability were previously released and are identified as SIDs 8369 and 8370.

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 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.