Nortel Threat Protection System SEU/Rule Update

Date: 01/10/2007

Software Files and File Names:

TPS 4.1 Series SEU#57	**TPS_Snort_Engine_Upgrade-57-vrt.sh**
TPS 4.5.1 Series SEU#57	**TPS_Snort_Engine_Upgrade-57-vrt.sh**
TPS 4.6 Series SEU #57	(Beta, un-released)

Rule Update Synopsis:

The Nortel Vulnerability Research Team (VRT) has discovered a serious vulnerability affecting Microsoft Outlook and is aware of a vulnerability affecting Adobe Acrobat Reader.

Details:

Microsoft Security Bulletin MS07-003:
The Nortel VRT has discovered a remotely exploitable vulnerability in Microsoft Outlook when it is used to process iCal calendar requests. iCal files may be used in meeting requests and can be sent to recipients using email. Included in an iCal request is time zone data that is used on the system to automatically populate the calendar in Outlook with the contents of the file.

An error in the processing of time zone data in a VEVENT record of an iCal file may allow a remote attacker to execute arbitrary code on a vulnerable system with the privileges of the current user. This may lead to the complete compromise of an affected host.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9841.

Adobe Acrobat Reader Plugin CVE-2007-0046:
The Adobe Acrobat Reader Plugin does not correctly process user-supplied input in the parameters supplied to a URI. This may allow a remote attacker to execute arbitrary code on an affected system.

Rules to detect attacks targeting this vulnerability are included in this release and are identifed as SIDs 9842 and 9843.

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.