Nortel Threat Protection System SEU/Rule Update

Date: 07/13/2006

This rules update is Snort Engine Update (SEU) #33. This update applies to all 4.1 and 4.5 models of the Defense Center and Intrusion Sensor.

Software Files and File Names:

TPS 4.1 Series SEU#33	**TPS_Snort_Engine_Upgrade-33-vrt.sh**
TPS 4.5.1 Series SEU#33	**TPS_Snort_Engine_Upgrade-33-vrt.sh**

07/13/2006 Rule Update Synopsis:

The Nortel VRT has learned of vulnerabilities affecting hosts using the Microsoft Operating System and hosts using the Linux 2.6 kernel.

Details:

Microsoft Security Bulletin MS06-035
The mailslot service is used on hosts using the Microsoft Operating System to handle messages between hosts on a domain.

An unchecked buffer in the mailslot server service may allow an attacker to overflow a fixed length buffer and execute code of their choosing on an affected host.

Rules to detect attempts to exploit this vulnerability are included in this rule pack and are identified as sids 7035 through 7046.

Microsoft Security Bulletin MS06-037
An Excel file containing a chart object and another additional object of any type with a large header length value, can be used to overflow a fixed length buffer and execute code of the attackers choosing on an affected host.

Rules to detect attempts to exploit this vulnerability are included in this rule pack and are identified as sids 7047 and 7048.

Linux hosts using the Netfilter module may be subject to a Denial of Service (DoS) condition when trying to process SCTP packets that do not contain chunks.

A rule to detect attempts to exploit this vulnerability is included in this rule pack and is identified as sid 7021.

WARNING: Nortel Threat Protection System customers must upgrade to 4.1.0.2 or 4.5.1 (as applicable) prior to applying SEU #33. Failure to apply this patch 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.