Nortel Threat Protection System SEU/Rule Update

Date: 04/10/2007

Software Files and File Names:

TPS 4.5.1 Series SEU#70	**TPS_Snort_Engine_Upgrade-70-vrt.sh**
TPS 4.6 Series SEU #70	**TPS_Snort_Engine_Upgrade-70-vrt.sh**

This update is SEU 70 for all models of the 4.6 and 4.5 series of the Defense Center and Intrusion Sensor.

Synopsis:

The TPS team is aware of vulnerabilities affecting hosts using Microsoft UPnP service and the Microsoft Agent.

Details:

Microsoft Security Bulletin (MS07-019):
Microsoft Universal Plug and Play does not correctly handle malformed HTTP requests. This may allow an attacker to overflow a buffer and execute code on a vulnerable host.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 10475

Microsoft Security Bulletin (MS07-020):
Microsoft Agent does not correctly handle malformed URLs. This may allow an attacker to cause a buffer overflow condition to occur and subsequently, execute code on an affected system.

Previously released rules will generate events when attempts are made to exploit this condition. These rules are identified as SIDs 4172 and 8846 through 8856. In addition, new rules are included in this release to detect attacks targeting this vulnerability and are identified as SIDs 10465 and 10474.

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.