NORTEL

Nortel Threat Protection System SEU/Rule Update 03/08/2006

Date: 03/08/2006

This rules update is Snort Engine Update (SEU) #16 for the 4.1 series and Rule Pack 46 for the 3.2 series of the Nortel Threat Protection System Defense Center and Intrusion Sensor. This rules update applies to the TPS 2070 Defense Center and all TPS 2x50/2x70 Intrusion Sensor models.

Software Files and File Names:

TPS 4.1 Series SEU#16	**TPS_Snort_Engine_Upgrade-16-vrt-sh**
TPS 3.2 Series Rule Pack#46	**Nortel_TPSRule_Pack-3.2.0-46.sh**

This update contains both engine (4.1 only) and rule updates.

Detection Engine Updates:

Note This engine update applies to SEU 16 for the v4.1 series of the Defense Center and Intrusion Sensor only. Previous versions are unaffected.

This release contains a fix for an issue where under certain conditions the frag3 preprocessor will not properly refragment stream data. This SEU also contains a number of other improvements to the detection engine, including performance upgrades and improved rule handling.

03/08/2006 Rule Update Synopsis:

The Nortel Threat Protection System Team has also added rules and improved detection capabilities as a result of ongoing research into vulnerabilities and in response to feedback regarding rule performance in certain situations.

Details:

Microsoft Security Bulletin MS05-027 A buffer overflow exists in the SMB (Server Message Block) Protocol implementation in Microsoft Windows 2000, Windows XP and Windows 2003 that allows attackers to cause a denial of service via a malformed request. Rules to detect attacks against this vulnerability are included in this rule pack and are identified as sids 5727 through 5783.

Apple Macintosh OS X suffers from a poorly designed use of resource forking for applications. It may be possible for an attacker to execute code of their choosing or execute system commands by exploiting the way in which OS X handles the opening of files determined to be safe. A rule to detect exploits against this vulnerability is included in this rule pack and is identified as sid 5713.

WARNING:

Nortel Threat Protection System customers must upgrade to 4.1.0.1 prior to applying SEU #16. Nortel Threat Protection System customers must upgrade to 3.2.0.3 or higher in order to utilize the enhanced rules in Rule Pack 46. Failure to apply these patches 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, 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.