Nortel Threat Protection System SEU/Rule Update 06/13/2006

Date: 06/13/2006

This rules update is Snort Engine Update (SEU) #29 for the 4.1.0.2 and 4.5.1 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#29	**TPS_Snort_Engine_Upgrade-29-vrt-sh**
TPS 4.5.1 Series SEU#29	**TPS_Snort_Engine_Upgrade-29-vrt-sh**

06/13/2006 Rule Update Synopsis:

Synopsis:

The Nortel VRT has learned of multiple vulnerabilities affecting Microsoft Internet Explorer, Apple Quicktime, Novell eDirectory, Sophos Anti-Virus and Symantec Anti-Virus products.

SEU 29 also contains a new version of the Nortel Rules Import tool. This new version fixes a problem concerning corrupted policies that may occur under some extraordinary circumstances.

Details:

Microsoft Internet Explorer contains a programming error in the way that it processes MIME HTML links (mhtml) which are commonly embedded in HTML email. The error in processing the links may allow a remote attacker to overflow a fixed length buffer and execute code of their choosing on the target system.

Rules to detect attacks against this vulnerability are included in this rule pack and are identified as sids 6509 and 6510.

Apple Quicktime fails to properly check user supplied data which may allow a remote attacker to overflow a fixed length buffer and execute code of their choosing on the target host.

Rules to detect attacks against this vulnerability are included in this rule pack and are identified as sids 6505 and 6506.

Novell eDirectory Server contains a vulnerability that may allow an attacker to overflow a fixed length buffer and execute code of their choosing on an affected server. The vulnerability exists in the iMonitor NDS server and may be exploited via a specially crafted uri to the service.

A rule to detect attacks against this vulnerability is included in this rule pack and is identified as sid 6507.

Sophos Anti-Virus fails to properly process Microsoft CAB files. A remote attacker may be able to leverage this vulnerability to execute code of their choosing on the target host or cause a denial of service (DoS) against the Sophos Anti-Virus process.

A rule to detect attacks against this vulnerability is included in this rule pack and is identified as sid 6504.

Symantec Anti-Virus Real-Time Scan Service suffers from a programming error that may allow a remote attacker to execute code of their choosing on an affected host.

A rule to detect attacks against this vulnerability is included in this rule pack and is identified as sid 6512.

WARNING: Nortel Threat Protection System customers must upgrade to 4.1.0.2 or 4.5.1 (as applicable) prior to applying SEU #28. 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.