NORTEL

Nortel Threat Protection System SEU/Rule Update

Date: 01/05/2007

Software Files and File Names:

TPS 4.1 Series SEU#56	**TPS_Snort_Engine_Upgrade-56-vrt.sh**
TPS 4.5.1 Series SEU#56	**TPS_Snort_Engine_Upgrade-56-vrt.sh**

Rule Update Synopsis:

The Nortel VRT is aware of multiple vulnerabilities affecting RealPlayer, Microsoft Outlook, Apple Quicktime, Yahoo Messenger and Symantec Veritas NetBackup. New rules have been introduced to provide coverage for exploitation attempts targeting these vulnerabilities.

Details:

Apple QuickTime RTSP Buffer Overflow CVE-2007-0015:
Apple QuickTime suffers from a programming error that may allow a remote attacker to overflow a fixed length buffer and execute code of their choosing on a vulnerable system. The condition is present in the processing of rtsp uri parameters.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9823.

Apple QuickTime Security Bypass CVE-2006-4965:
It may be possible for a remote attacker to execute arbitrary code by using a QuickTime Media Link (QTL) file. This file may contain elements that could call on external scripts to be executed on the vulnerable machine.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 9428 and 9430.

Apple QuickTime HREFTrack Scripting:
Apple QuickTime is prone to a scripting attack via the use of the HREFTrack parameter in a media file (.mov). A remote attacker could make use of this vulnerability to perform a cross site or cross zone scripting attack against a vulnerable machine.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9840.

Microsoft Outlook Denial of Service CVE-2006-6659:
Microsoft Outlook is prone to a Denial of Service (DoS) attack via the Recipient ActiveX control. An attacker would need to supply a malicious HTML file to be viewed using Microsoft Outlook.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 9668 through 9670.

RealNetworks RealPlayer Denial of Service CVE-2006-6847:
RealPlayer is prone to a Denial of Service (DoS) when supplied with a long argument via the ActiveX control that invokes RealPlayer in a browser session.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 9671 through 9673.

Symantec Veritas NetBackup Buffer Overflow CVE-2006-5822:
The Symantec Veritas NetBackup daemon suffers from a programming error that may allow a remote attacker to overflow a fixed length buffer and execute code of their choosing on an affected system.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 9813.

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.