Release Summary

Release Date: 23-January-2008
Purpose: This update is SEU 125 for all models of the 3D Sensor version 4.7, the 4.7 and 4.6 series of the Defense Center and Intrusion Sensor version 4.6.

Synopsis

The Nortel TPS team is aware of vulnerabilities affecting Microsoft Windows Media Player and Adobe Flash Player. This release also contains rules to address CVE entries CVE-2008-0236, CVE-2008-0237, CVE-2007-3847 and CVE-2008-0248.

Details

Microsoft Windows Media Player Buffer Overflow (CVE-2007-6401):
A buffer overflow condition in Microsoft Windows Media Player may be used by an attacker to execute code of their choosing on an affected system via a malicious .mp4 file.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 13316 through 13320.

Adobe Flash Player Input Validation Error (CVE-2007-6242):
Adobe Flash Player does not correctly validate user input when processing flash animation files. A remote attacker may use these vulnerabilities to execute code on an affected system.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 13300 and 13301.

Multiple other rule additions have been made to address vulnerabilities described in CVE entries CVE-2008-0236, CVE-2008-0237, CVE-2007-3847 and CVE-2008-0248.

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.