Threat Protection System
Snort Engine Update 126

Release Summary

Release Date: 29-January-2008
Purpose: This update is SEU 126 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 the Cisco Unified Communications Manager and SAP MaxDB.

Details

Cisco Unified Communications Manager Buffer Overflow (CVE-2008-0027):
A buffer overflow condition in the Certificate Trust List Provider service used by the Cisco Unified Communications Manager may allow a remote attacker to execute code on an affected system.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 13363.

SAP MaxDB Command Injection (CVE-2008-0244):
SAP MaxDB fails to correctly sanitize user-supplied input before passing the data to certain commands. A remote attacker may be able to inject commands to be executed on an affected system via the use of shell meta-characters.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 13356.

Other rules have been added to address the vulnerabilities described in CVE entries CVE-2007-5511, CVE-2007-4731, CVE-2007-6435 and CVE-2007-6335. Multiple rules have also been added to the spyware-put and web-client categories to provide further coverage for additional ActiveX vulnerabilities and spyware programs.

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.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support