Threat Protection System
Snort Engine Update 159

Release Summary

Release Date: 29-July-2008

Purpose: The SEU 159 (previous SEU–158) applies to:

- 3D Sensor Version: 4.7
- Defense Center Version(s): 4.7 and 4.6.0.2
- Intrusion Sensor Version(s): 4.6

Note: All SEU packages are cumulative. The installation of prior SEU packages is not required before installing the current package.

WARNING: The time taken to install the latest SEU will depend on the last time the 3D System was updated with an SEU. Installing SEUs weekly can help lessen the installation time. Additionally, SEUs require 50 Megabytes of free space in /tmp and 150 Megabytes of free space in /var to install successfully.

Synopsis:

The Nortel Threat Protection System team is aware of vulnerabilities affecting Sun Java Web Start, Oracle Database Server and DNS implementations.

Details:

Sun Java Web Start Buffer Overflow (CVE-2008-3111):
Sun Java Web Start contains programming errors that may allow a remote attacker to execute code on a vulnerable system.

A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1 and SID 13950.

Oracle Database Server Buffer Overflow (CVE-2008-2607):
Oracle Database Server contains programming errors that may allow a remote attacker to cause a Denial of Service (DoS) or a buffer overflow that may allow the attacker to execute code on a vulnerable system.

A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1 and SID 13951.

DNS Cache Poisoning (CVE-2008-1447):
The DNS protocol as implemented in many distributions may allow a remote attacker to spoof DNS traffic via cache poisoning techniques. In addition to the detection provided by SID 13667 for this vulnerability, the Nortel Threat Protection System team has added SIDs 13948 and 13949 to detect anomalous backscatter DNS traffic that would be generated during a DNS cache poisoning attack.

Additionally, as a result of ongoing research, the Nortel Threat Protection System team has added multiple rules to the spyware-put and backdoor rule sets to provide coverage for emerging threats from these technologies.

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