



Threat Protection System

Snort Engine Update 138

Release Summary

Release Date: 2-April-2008

Purpose: This update is SEU 138 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.

Note: All SEU packages are cumulative. The installation of prior SEU packages is not required before installing the current package. SEU 137 was issued internally and never made public. It is not necessary to install SEU 137 before installing SEU 138.

Synopsis

The Nortel TPS team has added multiple rules in the spyware-put and web-client categories to provide coverage for emerging spyware and ActiveX control threats.

Details

As a result of ongoing research, the Nortel TPS team has added multiple rules to the spyware-put and web-client rule sets to provide coverage for emerging threats from these technologies.

This release also contains an updated detection engine for the Nortel 3D System that includes the following features:

- A web interface for the DNS preprocessor that provides an alternative to the previous command line interface. This feature requires Version 4.7 or greater Nortel 3D System software.
- Support for GRE.
- Support for IP tunneling, for example, of IPv4 directly over IPv4.
- A CVS preprocessor that enables a rule keyword to test CVS traffic for malformed CVS entries which might be used by an attacker to force a heap overflow and execute malicious code on a CVS server.

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.

Copyright ©2007 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks Limited.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

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>