



Threat Protection System

Snort Engine Update 107

Release Summary

Release Date: 25-September-2007

Purpose: This update is SEU 107 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: If *all* rules are enabled in a policy object the policy may not correctly apply. This is a known issue.

Synopsis

The Nortel TPS team is aware of vulnerabilities affecting Firefox, ClamAV and the Apache HTTP Server.

Details

Firefox QuickTime Argument Injection (CVE-2007-5045):

A remote attacker may be able to execute commands via a QuickTime Media Link (QTL) file on systems using Firefox prior to version 2.0.7.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 12593.

ClamAV Command Execution (CVE-2007-4560):

The clamav-milter used in ClamAV prior to version 0.91.2 when run in black hole mode, may allow a remote attacker to execute commands via shell meta-characters.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 12592.

Apache HTTP Server Denial of Service (CVE-2007-1863):

The Apache HTTP Server (httpd), when caching is enabled and a threaded Multi-Processing Module (MPM) is used, is vulnerable to a Denial of Service (DoS) condition via a request using certain Cache-Control headers.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 12591.

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.

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>