



# Threat Protection System

## Snort Engine Update 168

### Release Summary

**Release Date:** 09-September-2008

**Purpose:** The SEU 168 (previous SEU-167) applies to:

- 3D Sensor Version: 4.8 and 4.7
- Defense Center Version(s): 4.8 and 4.7

### SEU Change Summary:

Component	Change
Total new rules	216
Total rule modifications	83
Policy change	Yes
Online help change	No
Detection Engine change	No
User Interface change	No

**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 multiple vulnerabilities affecting Microsoft products and SCADA systems.

### Details:

#### **Microsoft Security Advisory MS08-052:**

Vulnerability in Microsoft GDI may allow a remote attacker to execute code on a vulnerable system via specially crafted VML, GIF, BMP, EMF or WMF files. Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 3, SIDs 14259 through 14261.

Previously released rules will detect attacks targeting this vulnerability and are identified with GID 1, SIDs 3632 and 3634.

#### **Microsoft Security Advisory MS08-053:**

Windows Media Encoder 9 Series contains a vulnerability that may allow a remote attacker to execute code on an affected system via a specially crafted web page.

Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 3, SIDs 14255 through 14258.

**Microsoft Security Advisory MS08-054:**

Windows Media Player contains a vulnerability that may allow a remote attacker to execute code on an affected system via a specially crafted file streamed from a Windows Media Server.

Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 3, SIDs 14252 through 14254.

**Microsoft Security Advisory MS08-055:**

Microsoft Office contains a vulnerability that may allow a remote attacker to execute code on an affected system via a specially crafted OneNote URL.

A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 3, SID 14262.

**Citect CitectSCADA Stack Overflow CVE-2008-2639:**

The ODBC server service in Citect CitectSCADA and CitectFacilities contains a stack overflow vulnerability 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, SID 14265.

**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](http://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>