Threat Protection System
Snort Engine Update 201

Release Summary

Release Date: 10-February-2009

Purpose: The Snort Engine Upgrade (SEU) 201 (previous SEU–200) 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	20
Total rule modifications	46
Policy change	Yes
Online help change	No
Detection Engine change	No
User Interface change	No

Note: 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 Internet Explorer, Exchange, SQL Server and Visio.

Details

Microsoft Security Advisory MS09-002:
Microsoft Internet Explorer contains programming errors that may allow a remote attacker to execute code on a vulnerable system.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3, SIDs 15304 and 15305.

Microsoft Security Advisory MS09-003:
Microsoft Exchange contains programming errors that may allow a remote attacker to execute code or cause a Denial of Service (DoS) on an affected system.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3, SIDs 15301 and 15302.

Microsoft Security Advisory MS09-004:
A vulnerability in Microsoft SQL Server may allow a remote attacker to execute code on a vulnerable system. This issue may be exploited via the sp_replwritetovarbin stored procedure.

Rules to detect attacks targeting these vulnerabilities were included in a previous release and are identified with GID 1, SIDs 15127 through 15144.

Microsoft Security Advisory MS09-005:
Microsoft Visio contains programming errors that may allow a remote attacker to execute code on a vulnerable system via malformed Visio files.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3, SIDs 15298, 15299 and 15303.

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