Threat Protection System
Snort Engine Update 204

Release Summary

Release Date: 24-February-2009

Purpose: The Snort Engine Upgrade (SEU) 204 (previous SEU–203) 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	5
Total rule modifications	1
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

After additional research, Nortel Threat Protection System Team has added extra detection for a vulnerability affecting Adobe Acrobat and Acrobat Reader.

Details

Adobe Acrobat and Reader Buffer Overflow: Adobe Acrobat and Adobe Acrobat Reader contain a programming error that may allow remote attackers to execute code on a vulnerable system. The error occurs in the processing of files that use the JBIG2 compression routines on PDF files. This issue affects both products on Microsoft Windows, Linux and Mac OS X platforms.

A previously released rule to detect attacks targeting this vulnerability is included in this release and is now identified with GID 1, SID 15358. This rule was previously identified with GID 1, SID 15356.

Additionally, extra rules have been added to detect malicious pdf files being sent via email as well as a generic rule to detect any pdf files being sent via email.

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