Threat Protection System
Snort Engine Update 147

Release Summary

Release Date: 10-June-2008

Purpose: This update is SEU 147 for all models of the 3D Sensor version 4.7, the 4.7 and 4.6.0.2 series of the Defense Center and Intrusion Sensor version 4.6.

Note: 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.

Warning: The Nortel Threat Protection team is aware of vulnerabilities affecting the Microsoft Internet Explorer, Speech API, DirectX, WINS, Active Directory and the Windows operating system.

Synopsis

The Nortel Threat Protection team is aware of vulnerabilities affecting the Microsoft Internet Explorer, Speech API, DirectX, WINS, Active Directory and the Windows operating system.

Details

Microsoft Security Advisory (MS08-031):
Microsoft Internet Explorer contains a programming error that may allow a remote attacker to execute code on a vulnerable system.

A previously released rule will detect attacks targeting this vulnerability and is identified with GID 1 and SID 12279.

Microsoft Security Advisory (MS08-032):
The Microsoft Speech API contains a programming error that may allow a remote attacker to take control of a vulnerable system.

Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 3 and SIDs 13828 through 13833.

Microsoft Security Advisory (MS08-033):
Microsoft DirectX contains programming errors that may allow a remote attacker to execute code on a vulnerable system. These errors occur when DirectX attempts to parse malformed video and SAMI files.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3, SIDs 13823 and 13824.

Microsoft Security Advisory (MS08-034):
Microsoft WINS contains a programming error that may allow a remote attacker to take control of an affected system. The vulnerability occurs when WINS attempts to process malformed packet data.

A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 3 and SID 13826.

Microsoft Security Advisory (MS08-035):
Microsoft Active Directory is prone to a Denial of Service (DoS) attack that may be triggered by a remote attacker who is able to send malformed requests to the LDAP service.

A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 3 and SID 13835.

Microsoft Security Advisory (MS08-036):
The Microsoft Windows operating system is prone to a Denial of Service (DoS) attack that may be triggered by a remote attacker who is able to send malformed PGM packets to a vulnerable system.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3, SIDs 13827 and 13825.

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.