Threat Protection System
Snort Engine Update 130

Release Summary

Release Date: 12-February-2008
Purpose: This update is SEU 130 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: All SEU packages are cumulative. The installation of prior SEU packages is not required before installing the current package.

Synopsis

The Nortel TPS team is aware of multiple vulnerabilities affecting hosts using the Microsoft Windows operating system.

Details

Microsoft Security Bulletin (MS08-004):
Hosts using the Microsoft Windows operating system may be vulnerable to a Denial of Service (DoS) attack. The problem lies in the processing of DHCP requests provided to a host system by a server.

A shared object rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 3 and SID 13450.

Microsoft Security Bulletin (MS08-008):
Vulnerability in OLE Automation may present an attacker with the opportunity 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 and SIDs 13457 through 13460 and SID 13474.

Microsoft Security Bulletin (MS08-009):
Microsoft Word contains a vulnerability that may allow an attacker to execute code on an affected host.

A shared object rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 3 and SID 13469.

Microsoft Security Bulletin (MS08-010):
Microsoft Internet Explorer contains a number of memory corruption vulnerabilities that may allow a remote attacker to execute code on an affected system.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3 and SIDs 13451 through 13456.

Microsoft Security Bulletin (MS08-011):
Microsoft Works File Converter contains vulnerabilities that may allow an attacker to execute code on an affected system via a specially crafted Works file.

Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 3 and SIDs 13466 and 13472.

Microsoft Security Bulletin (MS08-012):
Microsoft Publisher contains two vulnerabilities that may allow a remote attacker to execute code on an affected system via specially crafted Publisher files.

Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 3 and SIDs 13470 and 13471.

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.

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