Threat Protection System
Snort Engine Update 217

Release Summary

Release Date: -09-April-2009

Purpose: The Snort Engine Upgrade (SEU) 217 (previous SEU–216) 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	0
Policy change	No
Online help change	No
Detection Engine change	No
User Interface change	Yes

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

This release contains a fix for a known issue in SEU 216, where intrusion policy validation can fail due to custom thresholding configurations. The following text relates to the changes made in SEU 216, as noted above SEUs are cumulative, SEU 217 also contains these changes.

Details

The DCE/RPC preprocessor now offers improved reassembly of fragmented DCE/RPC requests and improved desegmentation of SMB traffic containing DCE/RPC requests. The preprocessor now also alerts on anomalous behavior and evasion techniques in DCE/RPC data streams. Three new DCE/RPC rule keywords and new DCE/RPC arguments for the byte_test and byte_jump rule keywords add to the enhanced detection capabilities. Because of the new automatic preprocessor enabling feature described below, enabling a rule in an intrusion policy automatically enables the DCE/RPC preprocessor in the policy when the rule contains any of these new keywords and arguments. This SEU also deletes several thousand rules from the netbios rule category and adds or updates many new netbios rules for an overall net increase in protection and performance.
IMPORTANT: This SEU removes more than 5000 rules from the netbios rule category and replaces them with a much smaller number of rules, Nortel has taken care to ensure that your NetBIOS, SMB, DCE/RPC vulnerability coverage is not affected. This means that the vulnerabilities previously covered in your policies with hundreds of rules are now covered with one or two rules. You must import the SEU as described in the following steps to ensure that you are running the best possible netbios rule set.
NOTE: These changes only affect GID 1 rules, the shared object (GID 3) rules remain unaffected by the change to the preprocessor.

IMPORTANT: The SEU might not update a policy as expected if you import the SEU in one browser window when an intrusion policy page is open in another browser window.

1. Before importing the SEU, complete the following two tasks on the Rule State page in each intrusion policy:
   Note: Step 1.a is optional in policies that do not have any netbios rules currently enabled. Step 1.b is optional if the rule states of rules in the netbios category have not been changed from the default policy settings.
   1. Ensure that the "Allow SEUs to change existing rule states" check box is selected on the Rule State page in each intrusion policy.
   2. In order to maintain coverage, ensure that the replacement rules listed in the left column on this page are enabled if any of the replaced rule is in the right column are enabled.

      For example, in the first row, SID 10050 must be enabled if SID 10051 was enabled to maintain the same coverage.
2. For a complete list of these rule changes use this link.
   Note that some rules are completely replaced by the functionality that is now built into the DCE/RPC preprocessor.
3. After completing tasks a. and b. in each policy (if applicable), click Save, wait for the save to complete, and then exit the policy.
4. Import the SEU with the Rule State option on the Import SEU page set to "In the default state."
5. Re-apply each policy.

Note: Optionally, you can select the "Policy Reapply" option on the Import SEU page to automatically reapply your intrusion policies after the SEU import completes.
IMPORTANT: If these instructions are not followed then your policies may contain enabled rules in the deleted rules category. This will affect performance and will impact vulnerability coverage**.**

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