Nortel Threat Protection System SEU/Rule Update

Date: 04/09/2007

Software Files and File Names:

TPS 4.5.1 Series SEU#69	**TPS_Snort_Engine_Upgrade-69-vrt.sh**
TPS 4.6 Series SEU #69	**TPS_Snort_Engine_Upgrade-69-vrt.sh**

This update is SEU 69 for all models of the 4.6 and 4.5 series of the Defense Center and Intrusion Sensor.

Synopsis:

The TPS team is aware of vulnerabilities affecting Real Networks Helix Server, IBM Lotus SameTime ActiveX control and an issue with ipv6 traffic handling on OpenBSD systems. This release also contains an upgraded detection engine.

TPS has addressed a number of potential security-related issues in Snort as reported by customers, uncovered by internal investigations, and through third-party code audits.

Details:

OpenBSD IPv6 Fragmentation Overflow (CVE-2007-1365) and OpenBSD ICMP6 Denial of Service (CVE-2007-0343):
This release includes detection capabilities for attacks that attempt to exploit the IPv6 fragmentation overflow in OpenBSD-based operating systems.

Important Information about IPv6 Fragmentation Overflow Detection

Detection of traffic that attempts to exploit the IPv6 fragmentation overflow issue is enabled by default. If your Intrusion Sensor includes detection engines that are deployed inline on your network, the malicious traffic is dropped automatically.

For the TPS Intrusion Sensor 2050, 2070, 2150 & 2170, after you import this SEU and re-apply your intrusion policies as needed, traffic that attempts to exploit this vulnerability is detected by default. If you have deployed your sensor's detection engine inline, as mentioned previously, traffic is dropped automatically. To modify the default behavior, you must edit the user.conf file for the detection engine and add the following line:

```
config ipv6_frag: drop_bad_ipv6_frag off
```

Note: You must edit the user.conf file for each inline detection engine on the sensor. Instructions for creating and editing the user.conf file are included in the most recent version of the User Guide.

Note: The packet view in the web interface is not able to display IPv6 packets. However, you can use the packet view to download the pcap associated with malicious traffic and view it with the packet viewer of your choice. To display related events, search for intrusion events using the following GID:SID string in the Message field:

123:9, 123:10

Drill down to the packet view, expand the Event Information section, and select the "Download pcap file" option next to "Get Packet".

Real Networks Helix Server (CVE-2006-6026):
The Real Networks Helix Server fails to properly check user-supplied data to the application. This may allow a remote attacker to overflow a fixed length buffer and execute code on a vulnerable host.

A rule to detect attacks targeting this vulnerability is included in this release and is identified as SID 10407.

IBM Lotus SameTime (CVE-2007-1784):
IBM Lotus SameTime fails to properly process user-supplied input. This may allow an attacker to load DLL files and execute code by supplying suitable arguments to the loadLibrary function.

Rules to detect attacks targeting this vulnerability are included in this release and are identified as SIDs 10412 through 10417.

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.