NORTEL

Nortel Threat Protection System SEU/Rule Update

Date: 07/10/2006

This rules update is Snort Engine Update (SEU) #32. This update applies to all 4.1 and 4.5 models of the Defense Center and Intrusion Sensor.

Software Files and File Names:

TPS 4.1 Series SEU#32	**TPS-Snort-Engine-Upgrade-32-vrt-sh**
TPS 4.5.1 Series SEU#32	**TPS-Snort-Engine-Upgrade-32-vrt-sh**

07/10/2006 Rule Update Synopsis:

The Nortel Virtual Response Team is aware of a number of vulnerabilities affecting several Web browsers, including Internet Explorer and Firefox. This rule pack contains a number of rules to detect these issues.

Details:

The Nortel Virtual Response Team is aware of a number of vulnerabilities affecting several Web browsers, including Internet Explorer and Firefox. This rule pack contains a number of rules to detect these issues.

These rules are identified as sids 7003 through 7018.

This release also contains an improved version of the detection engine with better performance and minor bug fixes.

List of modified and deleted rules:

New Rules:
7003 - WEB-CLIENT ADODB.Recordset ActiveX function call access (web-client.rules)
7004 - WEB-CLIENT Internet.HHCtrl.1 ActiveX function call access (web-client.rules)
7005 - WEB-CLIENT OutlookExpress.AddressBook ActiveX function call access (web-client.rules)
7006 - WEB-CLIENT ASControls.InstallEngineCtl ActiveX function call access (web-client.rules)
7007 - WEB-CLIENT AxDebugger.Document.1 ActiveX function call access (web-client.rules)
7008 - WEB-CLIENT DirectAnimation.DAUserData ActiveX function call access (web-client.rules)
7009 - WEB-CLIENT DirectAnimation.StructuredGraphicsControl ActiveX function call access (web-client.rules)
7010 - WEB-CLIENT HtmlDlgSafeHelper.HtmlDlgSafeHelper.1 ActiveX function call access (web-client.rules)
7011 - WEB-CLIENT HtmlDlgSafeHelper.HtmlDlgSafeHelper ActiveX function call access (web-client.rules)
7012 - EB-CLIENT Internet.PopupMenu.1 ActiveX function call access (web-client.rules)

7013 - WEB-CLIENT Microsoft.ISCatAdm ActiveX function call access (web-client.rules)
7014 - WEB-CLIENT NMSA.ASFSourceMediaDescription.1 ActiveX function call access (web-client.rules)
7015 - WEB-CLIENT NMSA.MediaDescription ActiveX function call access (web-client.rules)
7016 - WEB-CLIENT Object.Microsoft.DXTFilter ActiveX function call access (web-client.rules)
7017 - WEB-CLIENT RDS.DataControl ActiveX function call access (web-client.rules)
7018 - WEB-CLIENT Sysmon ActiveX function call access (web-client.rules)

Updated rules:
1951 - RPC mountd TCP mount request (rpc.rules)

WARNING: Nortel Threat Protection System customers must upgrade to 4.1.0.2 or 4.5.1 (as applicable) prior to applying SEU #32. Failure to apply this patch will result in sensor failure when installing these rules.

Snort Engine Updates: In Threat Protection System v4.1, Snort Engine Updates (SEUs) replace 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.