SECURITY ADVISORY
FROM PATTON ELECTRONICS

Contact Information
Patton Electronics Co.
7622 Rickenbacker drive
Gaithersburg, MD 20879
Phone +1-301-975-1000
Fax +1-253-663-5693
support@patton.com
www.patton.com

Potential Security Vulnerabilities Identified in Simple Network Management Protocol (SNMP)

Revision 1.0
For Public Release March 7, 2002

Last Updated March 7, 2002

Summary

The CERT Coordination Center (CERT/CC) has issued a broad-based Alert to the technology industry regarding potential security vulnerabilities identified in the Simple Network Management Protocol (SNMP). Patton is working with CERT to assess and address this issue.

Vulnerabilities have been reported in multiple vendors' SNMP implementations. These vulnerabilities may allow unauthorized privileged access, denial-of-service attacks, or cause system instability. If your site uses SNMP in any capacity, the CERT/CC encourages you to read this advisory and follow the advice provided in the *Solutions* section.

The following provisions recommended by CERT and Patton Electronics Company should be employed in the operation of Patton's chassis-based RAS.

In addition to this advisory, we recommend reading the following FAQ available at

http://www.cert.org/tech_tips/snmp_faq.html

It is very important that you take the steps described in this document to address SNMP security vulnerabilities. As a Patton customer, our Technical Services Team is available to help you implement the recommended configuration changes.

Patton Technical Support contact info:

Tel: **+1 301-975-1007**

Fax: **+1 253-663-5693**

E-Mail: support@patton.com

WWW: http://www.patton.com/support

Products Affected

Most of Patton's products are Layer-1 or Layer-2 devices. As such, they are not susceptible to upper-layer attacks. Patton Electronics' chassis-based Remote Access Server (RAS) products—which are Layer-3 Internet appliances—are equipped with SNMP. The following models of Patton RAS servers employ SNMP V1.

- Model 2800
- Model 2810
- Model 2860
- Model 2960 16 Port RAS
- Model 2960 24 Port RAS
- Model 29660 30 Port RAS
- Model 2960 48 Port RAS
- Model 2960 60 Port RAS
- Model 2996 96 Port RAS
- Model 2996 120 Port RAS

Initial Determination

The Patton technical support team performed initial testing using *Solarwinds SNMP Brute Force Attack* software with a free-running batch file. Test results indicated that the Patton RAS products are not vulnerable to SNMP attacks.

The free-running batch file used in the test sent 19,000 GET requests, invalid OID requests, and improper community strings every 5 seconds for several hours. The Patton RAS under test logged over 3.5 million SNMP transactions without compromised operation. Figure 1 shows the results of the test and demonstrates the Patton RAS's ability to withstand a serious SNMP attack.

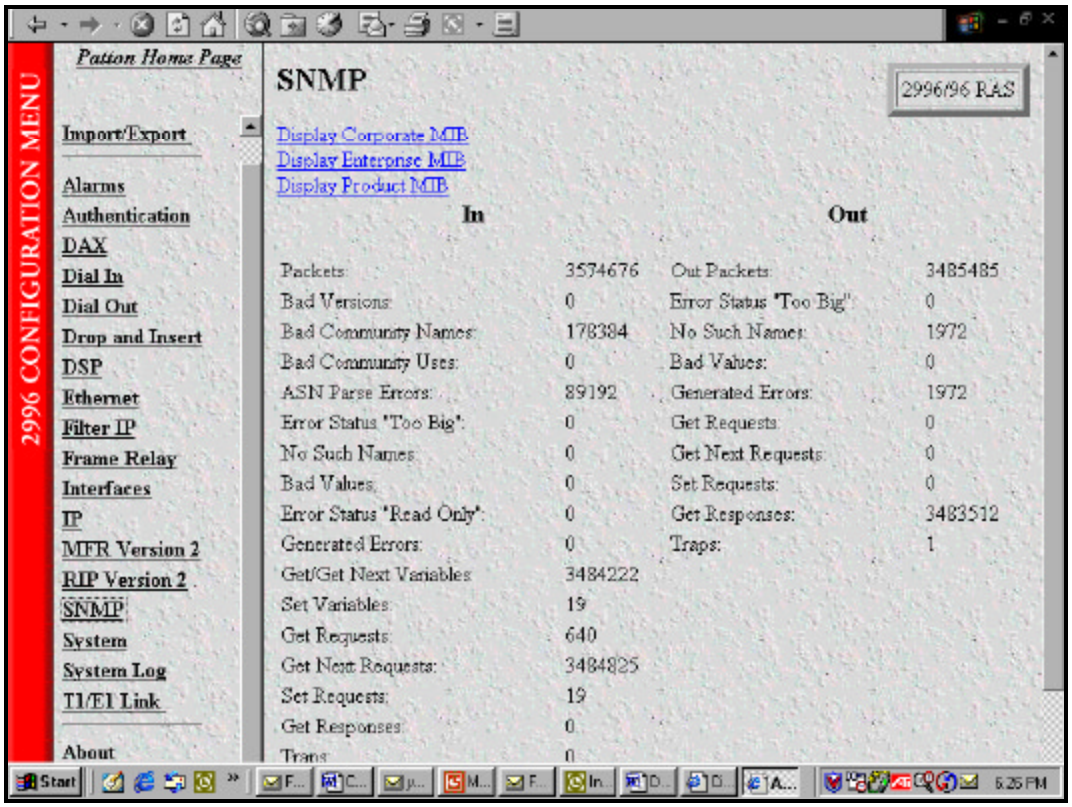

Figure 1

Using Patton's web-based management system, under the SNMP page shown in Figure 1, Network Managers can identify possible denial-of-service (DOS) attacks by monitoring the following items:

- Number of inbound packets ("Packets In")
- Bad Community Names
- Bad Community Uses
- Error Status "Too Big"

Prevention

Dial-in Users

The Patton RAS software suite enables filters to be applied to dial-in users that will prevent any type of IP access to the RAS. Creating filters for this purpose is sound practice for any installation and highly recommended by Patton. For additional information about using filters in the Patton RAS click on the link below to download our IP Filters overview.

www.patton.com/technotes/filter_ip.pdf

The diagram below shows the Filter IP window of the RAS management software. By clicking on the Filter IP link (see highlight in Figure 2 for link location) you can view the *Direction*, *Action*, *Destination IP*, and *Default for Dial-in* settings recommended by Patton.

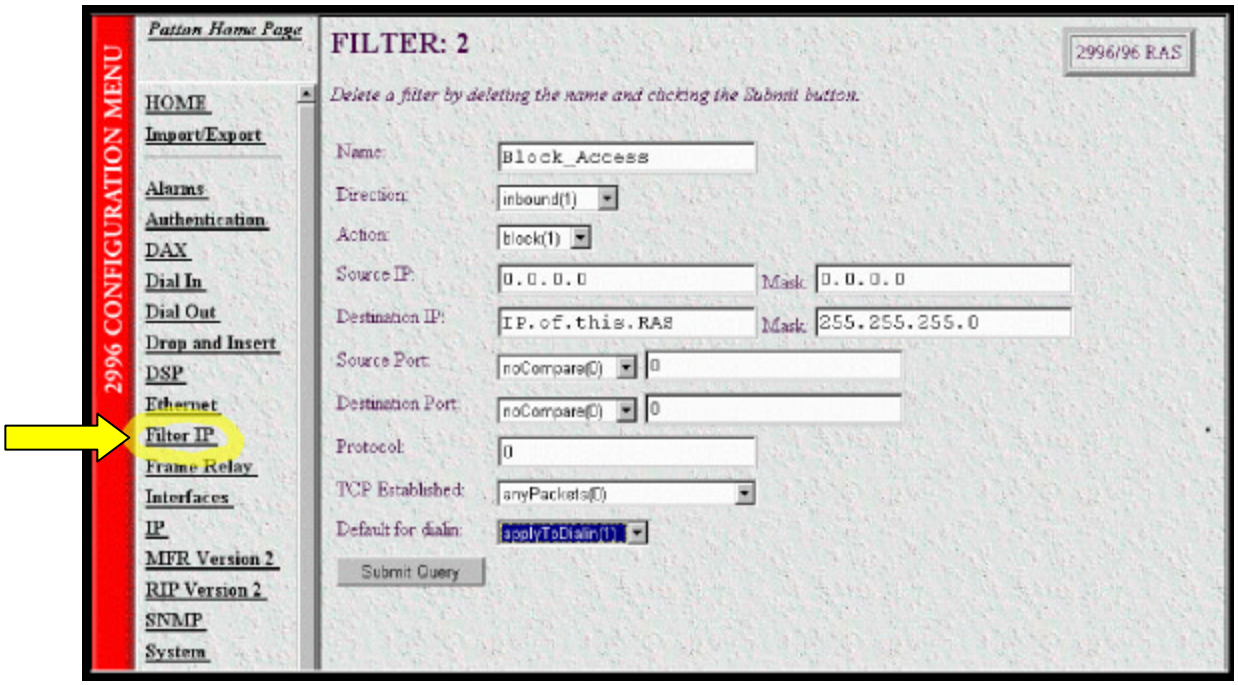

Figure 2

Ingress Network Protection

You can further limit SNMP vulnerabilities by blocking access to SNMP services at the network perimeter or *firewall*. This is known as *ingress filtering*.

Ingress filtering manages the flow of traffic as it enters a network that is under your administrative control. Servers are typically the only machines that need to accept inbound traffic from the public Internet. In the typical network operation of many sites, there are few reasons for external hosts to initiate inbound traffic to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services.

For SNMP, ingress filtering of the following ports listed below can prevent attackers outside of your network from impacting vulnerable devices in the local network that are not explicitly authorized to provide public SNMP services.

SNMP	**161/tcp**	**#Simple Network Management Protocol (SMNP)**
SNMP	**162/tcp**	**#SNMP system management message**

SNMP-enabled products ship with default community strings for read-only access and for read-write access. For security reasons, Patton Electronics recommends—as with any default access control mechanism—that network administrators change their default community strings to something of their own choosing with a 10-digit combination of numbers and letters. The community strings are encrypted, but even a 10-digit string of mixed numbers and letters is subject to eventual discovery by determined packet sniffing attacks. Therefore, you should change your community strings on a regular (bimonthly, for example) basis.

Disabling the web interface in a Patton RAS provides additional security by keeping HTTP requests from being processed

For further information related to the Patton remote access product line, contact our Technical Services Team at:

Tel: **+1 301-975-1007**

Fax: **+1 253-663-5693**

E-Mail: support@patton.com

WWW: http://www.patton.com/support