Global Information Assurance Certification Paper

Microsoft Windows 2000 Operating System SNMP Vulnerabilities

Terrence V. Lillard
December 11, 2000

Simple Network Management Protocol (SNMP) is a mechanism used for remote monitoring and management of network devices likes hubs, routers, bridges, as well as servers and workstations. SNMP is divided into the two components listed below:

- **SNMP management system.** Any computer running SNMP management software is an SNMP management system. The SNMP management system sends information and update requests to an SNMP agent. The management software application does not need to run on the same host as the SNMP agent. The SNMP management system requests information from a managed computer, called an SNMP agent, such as the amount of hard disk space available or the number of active sessions. The management system can also initiate a change to an agent's configuration.

- **SNMP agent.** Any computer running SNMP agent software is an SNMP agent The SNMP agent responds to management system requests for information. The SNMP Service can be configured to determine which statistics are tracked and which management systems are authorized to request information.

The Microsoft Windows 2000 Operating System was designed with a SNMP Service, though not installed by default, which functions as SNMP Agent software. The Microsoft Windows 2000 Operating System implements SNMP versions 1 and 2C. These versions are based on industry standards that define how network management information is structured, stored, and communicated between agents and management systems for TCP/IP-based networks. The Windows 2000 Operating System SNMP Agent Service responds to information requests from one or multiple management systems. In general, Windows 2000 Operating System SNMP agents do not originate messages, but only respond to them. This response occurs via SNMP agent-initiated trap communications.

The implementation of SNMP architecture is based upon the Management hosts and agents belong to a SNMP community, which is a collection of hosts grouped together for administrative purposes. This collection of SNMP hosts and agents can be secured within a community by allowing only management systems and agents within the same community to communicate. Communities are identified by community names that are assigned during implementation. A SNMP Management host can belong to multiple communities at the same time, but a SNMP Agent cannot accept a request from a management system outside its list of acceptable community names. The role of community names is very critical in the implementation of the SNMP service security properties. While there is no relationship between community names and domain or workgroup names, SNMP community names represent a shared password for groups of

network hosts, and should be selected and defined, as you would change any password protection system.

During the installation of the Microsoft Windows 2000 Operating System SNMP Service, incorrect permissions assigned to the Microsoft Windows 2000 Operating System SNMP Service registry key parameters listed below. As a result, a person can access the parameter information.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters

This vulnerability, which allows a person access the parameter key information, can be used to perform the following actions:

1. Create a community consisting solely of their local machine, in order to gain the ability to take administrative actions on it.

2. Obtain information about already-existing communities that the machine is a member of, and pose as a legitimate SNMP manager in order to monitor or reconfigure devices in the community. To perform these tasks, the agent uses the following messages:

SNMP Message	Description
Get	The basic SNMP request message. Sent by an SNMP management system, it requests information about a single MIB entry on an SNMP agent. For example, the amount of free drive space.
Get-next	An extended type of request message that can be used to browse the entire tree of management objects. When processing a Get-next request for a particular object, the agent returns the identity and value of the object, which logically follows the object from the request. The Get-next request is useful for dynamic tables, such as an internal IP route table.
Set	If write access is permitted, this message can be used to send and assign an updated MIB value to the agent.
Getbulk	Requests that the data transferred by the host agent be as large as possible within given restraints of message size. This minimizes the number of protocol exchanges required to retrieve a large amount of management information. The maximum message size should not be larger than the path maximum transmission unit (MTU), the largest frame size allowed for a single frame on your network, or fragmentation can occur.
Trap	An unsolicited message sent by an SNMP agent to an SNMP management system when the agent detects that a certain type of event has occurred locally on the managed host. The SNMP management console that receives a trap message is known as a trap destination. For example, a trap message might be sent on a system restart event.

This vulnerability applies to the Microsoft Windows 2000 Operating System. The resolution to this vulnerability is to apply the correct permissions to the following registry keys, as listed below:

Hive	Key	Permission
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet	Services\SNMP\Parameters\ PermittedManagers	Administrators, System, Creator Owner: Full
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet	Services\SNMP\Parameters\ ValidCommunities	Administrators, System, Creator Owner: Full

References:

- Microsoft Corporation. "SNMP Microsoft Security Bulletin (MS00-096): Frequently Asked Questions " http://www.microsoft.com/technet/security/bulletin/fq00-096.asp, December 2000

- Microsoft Corporation. "Microsoft Security Bulletin (MS00-096): Tool Available for "SNMP Parameters" Vulnerability", http://www.microsoft.com/technet/security/bulletin/MS00-096.asp, December 6, 2000.

- Microsoft Corporation. "Q266794: Windows 2000 SNMP Registry Entries Are Saved in Plain Text Format and Are Readable". December 6, 2000

- Microsoft Corporation. "WQ200885: How to Troubleshoot SNMP Security Issues". October 20, 2000