Software Engineering Institute
Carnegie Mellon University

Simple Network Management Protocol (SNMP) Vulnerabilities Frequently Asked Questions (FAQ)

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 Introduction

This FAQ is related to the CERT Advisory CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP).

2 Frequently Asked Questions

What is SNMP?

The Simple Network Management Protocol (SNMP) is the most popular protocol in use to manage networked devices. SNMP was designed in the late 80's to facilitate the exchange of management information between networked devices, operating at the application layer of the ISO/OSI model. The SNMP protocol enables network and system administrators to remotely monitor and configure devices on the network (devices such as switches and routers). Software and firmware products designed for networks often make use of the SNMP protocol. Support for SNMP is available on a multitude of systems, including, but not limited to,

- Core Network Devices (Routers, Switches, Hubs, Bridges, and Wireless Network Access Points)
- Operating systems (on nearly all architectures)
- Consumer Broadband Network Devices (Cable Modems and DSL Modems)
- Consumer Electronic Devices (Cameras and Image Scanners)
- Networked Office Equipment (Printers, Copiers, and FAX Machines)
- Network and Systems Management/Diagnostic Frameworks (Network Sniffers and Network Analyzers)
- Uninterruptible Power Supplies (UPS)
- Networked Medical Equipment (Imaging Units and Oscilloscopes)
- Manufacturing and Processing Equipment

How is SNMP vulnerable?

The vulnerabilities affect both manager and agent software (see "What are managers and agents?" for an explanation of these terms). Vulnerabilities in both managers and agents include denial-of-service conditions, format string vulnerabilities, and buffer overflows. Some of the vulnerabilities do not require the malicious packet to use the proper community string (see "What is a community string and how is it used?"). Several of the more serious vulnerabilities allow the execution of arbitrary code by a remote unauthenticated attacker. Refer to CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html) for a detailed description of the vulnerabilities.

Is our network or system in danger of attack?

Because of the relatively large number of products that support SNMP, it is unlikely that our list of affected products is comprehensive. Therefore, if you use products that support SNMP, we encourage you to first refer to CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html) for a partial list of affected vendors and products. If your vendor(s) are not listed you should contact them directly for more information to ensure your system is protected.

What can happen if we are attacked?

Exploitation of these vulnerabilities can cause denial-of-service conditions, service interruptions, and in some cases will allow an attacker to gain unauthorized, privileged access to the affected device. Effects for some specific products can be found in CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html). Contact your vendor(s) for additional information on other products.

How can we protect our network or system?

A number of steps can be taken to improve the security of systems relying on SNMP:

- Apply a patch from your vendor.
- Disable all nonessential SNMP software.
- Filter SNMP access to managed devices to ensure the traffic originates from known management systems.
- Filter SNMP services at your network perimeter (ingress/egress filtering).
- Change SNMP community strings from their defaults.
- Segregate network management traffic onto a separate network.

Refer to CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html) for more details and the most recent information regarding recommended solutions.

Are there any alternatives to using SNMP?

Although there aren't many practical alternatives to SNMP, there are steps that administrators can take to better secure their systems that use SNMP. See the "How can we protect our network or system?" section above or refer to CERT Advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html) for more information.

Do these vulnerabilities affect home users?

Most home users are not directly affected by these vulnerabilities. However, home users with more advanced configurations may be at risk. If you use one or more of the following in your home system or network, additional steps might be necessary to ensure protection:

- Microsoft Windows operating systems with SNMP services enabled
- advanced operating systems (e.g., Linux or other Unix operating systems)
- network-based router appliances
- network-based firewall appliances
- wireless Ethernet (802.11a/b) access points

Note that in many cases SNMP services are not enabled by default, so merely using one or more of the products above does not mean that you are definitely vulnerable. Home users with one or more of the above technologies in use on their home networks are encouraged to refer to CERT

advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html) for a partial list of affected vendors and products. If your vendors are not listed you should contact them directly for more information to ensure your system is protected.

What are managers and agents?

SNMP is built around the concept of "managers" and "agents." Manager software (commonly installed on a network management system) makes requests to agent software running on a host or device to gather data on the operational status, configuration, or performance statistics of that system (polling). Some agents allow configuration parameters to be changed by managers, while others provide read-only statistics and configuration information. Additionally, agents can generate ad-hoc messages to manager systems to inform them of unusual events (traps).

What is a community string and how is it used?

The community string (a.k.a. community name) provides a weak authentication mechanism to the SNMP protocol. Agents can be configured to allow read-only, read-write, or no access to their parameters based on the community string in a request. Community strings are passed in clear text in SNMP messages, so they can be easily sniffed and are therefore insufficient for authenticating legitimate manager requests.

Note that many of the vulnerabilities described in CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html) do **not** require an attacker to know the configured community strings in order to exploit the vulnerability.

What protocols/ports does SNMP use?

SNMP uses 161/udp for general purpose (request/response) communications, and 162/udp for traps. Additionally, the SNMP multiplexing protocol (smux, defined in RFC1227 http://www.ietf.org/rfc/rfc1227.txt) uses 199/tcp. Another SNMP extension, the AgentX protocol (RFC2741, http://www.ietf.org/rfc/rfc2741.txt) uses 705/tcp.

Where can I find the specifications for SNMP?

The current SNMPv1 standard is defined in the Internet Engineering Task Force (IETF) STD0015 / RFC1157 (http://www.ietf.org/rfc/rfc1157.txt). There are also a number of draft and proposed standards for SNMPv2 and SNMPv3. Refer to IETF STD0001 / RFC3000 (http://www.ietf.org/rfc/rfc3000.txt) for the current status of the various SNMP-related RFCs.

Where can I find additional information about SNMP?

The comp.protocols.snmp FAQ may be found at http://www.faqs.org/faqs/snmp-faq/part1/ and http://www.faqs.org/faqs/snmp-faq/part2/.

There are a number of SNMP-related Working Groups in the "Operations and Management" area of the IETF (http://www.ietf.org/).

Has the CERT/CC received any reports of SNMP scanning?

As of 9:25 EST (UTC-0500) February 12, 2002, we have received reports of scanning for SNMP services related to these vulnerabilities and are working to verify.

I have detected scanning of my network or systems for SNMP. Should I report that to the CERT/CC?

If you have detected scanning for SNMP services on your network, you should first determine whether this scanning has led to a compromise or not. You may wish to refer to our Intruder Detection Checklist (http://www.cert.org/tech_tips/intruder_detection_checklist.html) for additional tips on determining whether a compromise has occurred.

Once you are certain that no compromise has occurred and the impact was limited to scanning only, you are encouraged to report this activity to the CERT/CC using our Incident Reporting Form, available at http://www.cert.org/reporting/incident_form.txt.

Reporting scanning activity to the CERT/CC will help us better assist you, and allow us to relate ongoing intruder activities. This also provides us a better overview of trends in attack profiles and provides input for other CERT documents such as advisories and summaries. We prefer that Incident Reporting Forms be sent to us via email to cert@cert.org.

Has the CERT/CC received any reports of exploitation of these vulnerabilities?

As of 9:25 EST (UTC-0500) February 12, 2002, we have received reports of exploitation of SNMP services related to these vulnerabilities and are working to verify them.

An intruder has exploited these SNMP vulnerabilities on my system. What should I do?

As described in CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html), exploitation of these SNMP vulnerabilities can cause denial-of-service conditions, service interruptions, and in some cases will allow an attacker to gain unauthorized, privileged access to the affected device(s).

If you suspect that your system may have been compromised, you may wish to refer to our Intruder Detection Checklist (http://www.cert.org/tech_tips/intruder_detection_checklist.html). Once you have confirmed that a compromise has occurred, please refer to our Steps for Recovering from a UNIX or NT System Compromise (http://www.cert.org/tech_tips/root_compromise.html)

Regardless of whether the exploitation resulted in system compromise or denial-of-service, we would appreciate it if you would complete and return an Incident Reporting Form as this will help us better assist you, and allow us to relate ongoing intruder activities. This also provides us a better overview of trends in attack profiles and provides input for other CERT documents such as advisories and summaries. We prefer that Incident Reporting Forms be sent to us via email to cert@cert.org. The Incident Reporting Form is available from http://www.cert.org/reporting/incident_form.txt.

I am not a vendor, but I use or otherwise have first-hand knowledge of an SNMP product that is vulnerable, but it is not on the CERT/CC's list. Should I report that to the CERT/CC?

If you have first-hand knowledge of an SNMP product that is vulnerable to either of these vulnerabilities, and that product or vendor is not listed in CERT advisory CA-2002-03 (http://www.cert.org/advisories/CA-2002-03.html), you are encouraged to contact us using our Product Vulnerability Reporting Form. This form can be found at http://www.cert.org/reporting/vulnerability_form.txt.

Please send the completed form to cert@cert.org with VU#617947 in the subject line.

Our company manufactures a product that uses SNMP, and we think it might be vulnerable, but we are not sure. How can we get more information on these vulnerabilities?

The CERT/CC encourages any vendors whose products are affected (whether vulnerable or not) by these or any other security vulnerabilities to contact us so that we can establish a working relationship on this and any future issues that may arise. If you are authorized to represent your organization on this issue, please contact the CERT/CC via our hotline at +1 412-268-7090. CERT/CC personnel answer 8:00 a.m.- 5:00 p.m. EST(GMT-5) / EDT(GMT-4) on working days; they are on call for emergencies during other hours and on weekends and holidays.

Our company manufactures a product that uses SNMP, and we know it to be affected by these vulnerabilities, but we are not listed in any of your vendor statements. How can we get added to your list of vendors?

The CERT/CC encourages any vendors whose products are affected (whether vulnerable or not) by these or any other security vulnerabilities to contact us so that we can establish a working relationship on this and any future issues that may arise. If you are authorized to represent your organization on this issue, please contact the CERT/CC via our hotline at +1 412-268-7090. CERT/CC personnel answer 8:00 a.m.- 5:00 p.m. EST(GMT-5) / EDT(GMT-4) on working days; they are on call for emergencies during other hours and on weekends and holidays.

Our company manufactures a product that uses SNMP, but we know it is not affected by these vulnerabilities. Nonetheless, we are being swamped with calls to our help desk about this issue. We are not currently listed in any of your vendor statements, but we'd like to be. How can we get added to your list of vendors?

The CERT/CC encourages any vendors whose products are affected (whether vulnerable or not) by these or any other security vulnerabilities to contact us so that we can establish a working relationship on this and any future issues that may arise. If you are authorized to represent your organization on this issue, please contact the CERT/CC via our hotline at +1 412-268-7090. CERT/CC personnel answer 8:00 a.m.- 5:00 p.m. EST(GMT-5) / EDT(GMT-4) on working days; they are on call for emergencies during other hours and on weekends and holidays.

Who is OUSPG?

The Oulu University Secure Programming Group (OUSPG) is an academic research group located at Oulu University in Finland. The purpose of this research group is to test software for vulnerabilities.

History has shown that the techniques used by the OUSPG have discovered a large number of previously undetected problems in the products and protocols they have tested. Earlier this year, the OUSPG produced a comprehensive test suite for evaluating implementations of the Lightweight Directory Access Protocol (LDAP). This test suite was developed with the strategy of abusing the protocol in unsupported and unexpected ways, and it was very effective in uncovering a wide variety of vulnerabilities across several products. This approach can reveal vulnerabilities that would not manifest themselves under normal conditions.