



Security Overview - Vulnerabilities in SNMP

The recent highlighting by CERT (<http://www.cert.org/advisories/CA-2002-03.html>) of security vulnerabilities in SNMP means that network professionals have another item on their 'to do' list.

For those of you not familiar with SNMP we have summarised some details below about SNMP, how it works and the security risk.

Kenson Network Engineering Limited is uniquely placed to assist you and your organisation with this problem. We have many years' experience in network management and have developed our security services to complement this area. These are exactly the skills needed to deal with this particular risk.

If, after reading the following information, you would like an informal discussion, contact one of our technical specialists on 01285 647900.

What Is SNMP?

SNMP is not a single standard or protocol but rather a growing set of specifications covering network management in the TCP/IP environment.

As the name suggests SNMP is a simple tool for network management. It defines a limited, easily implemented database of management information and a protocol to enable remote manipulation of the database.

The main strength of SNMP is its simplicity. It is easy to implement and consumes modest processor and network resources. The straightforward structure of the protocol

Kenson Network Engineering Ltd

Corinium House
Units 101/102
Cirencester Business Park
Love Lane
Cirencester
Gloucestershire
GL7 1XD

T: +44 (0)1285 647900
F: +44 (0)1285 643686
E: enquiries@kenson.co.uk
W: www.nut.eu.com/kenson

Nu Technologies

Kenson are part of the
Nu Technologies Group

and the information database make it easy for vendors to achieve interoperability. Simplicity is also SNMP's main weakness as once users become used to the basic monitoring and control features they find they want more efficiency, more functionality and especially more security.

One of the most notable deficiencies in the original SNMP specification, issued in August 1988, was the difficulty in monitoring networks as opposed to nodes on the network. In response to this an extension to the SNMP information database was issued in November 1991 in the form of the remote network monitoring (RMON) MIB.

How is it Used?

The use of SNMP has three distinct elements to it:

- A manager
- An agent
- A protocol, which controls the exchange of information between a manager and an agent.

A manager is a set of applications, which reside within a network management station. The management station collects data from agents and performs the analytical functions required to monitor and control the network. It is the user interface for the Network Administrator.

An agent is a software program, transparent to users, housed within a network device (such as a host, router or switch). The agent collects statistics about the device and provides access to that information by the management station.

The manager and agent exchange network management information with each other using the SNMP protocol over a UDP/IP link.

The Security Risk

SNMP is designed to provide management of network infrastructure so is an ideal channel to compromise if an entity wishes to cause disruption to your IT operation. On February 12 2002 CERT reported that a variety of vulnerabilities had been reported in numerous vendors' implementations of the SNMP protocol.

These vulnerabilities may cause unstable behaviour, unauthorised access or denial-of-service incidents if exploited. The actual manifestation of the vulnerability varies from item to item and manufacturer to manufacturer.

There are a variety of mitigating actions that can be taken including:

- Disabling SNMP where not needed.
- Changing passwords (community strings).
- Filtering SNMP traffic out at routers or firewalls.
- Applying vendor patches

Care needs to be taken in mitigating the risk that the use of the SNMP in running your network is not compromised. SNMP is an important part of network and IT service delivery in many organisations and altering its deployment can have significant impact on you network operations capability.

As discussed above SNMP can run on a huge range of network and IT hardware and is often installed by default on many systems. Thus the true extent of SNMP use or deployment in a network is often unknown.

Recommendations

Kenson Network Engineering Limited recommends the following actions as a minimum response:

- Audit your network for SNMP use
- Decide if the use of SNMP is valid in all instances
- Identify which of your systems and hardware have manufacturer recommended patches available that address this vulnerability

Further action should be planned based on the information collected.

Kenson Network Engineering Ltd

Corinium House
Units 101/102
Cirencester Business Park
Love Lane
Cirencester
Gloucestershire
GL7 1XD

T: +44 (0)1285 647900
F: +44 (0)1285 643686
E: enquiries@kenson.co.uk
W: www.nut.eu.com/kenson



Kenson are part of the
Nu Technologies Group