GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

**Your Greatest Strength can become your Greatest Weakness:
Simple Network Management Protocol Vulnerabilities**

Summary

According to the recent press coverage, multiple
vulnerabilities have been discovered in the widely used
Simple Network Management Protocol (SNMP). This paper will
discuss some of the major vulnerabilities discovered in SNMP
and their potential impact as well as some of the major
vendors affected by these vulnerabilities and possible
solutions and alternatives that can be implemented to
protect systems from these vulnerabilities.

Background

Simple Network Management Protocol (SNMP) was developed in
the late 1980's by the Internet Engineering Task Force to
provide a standard network management protocol to manage
network devices. As its name implies, simplicity was the
focus of this protocol as it was being developed. SNMP's
ultimate goal was interoperability so it could be widely
used across most all platforms and devices. Its developers
accomplished this goal, as demonstrated by its use in almost
every major networking product on the market. SNMP's
simplicity was designed to minimize the overhead needed to
run such a protocol and keep the complexity of network
management to a minimum.

SNMP is a request-reply protocol that runs over UDP (User
Datagram Protocol) on ports, paths into and out of a
computer or network device, 161 and 162. The protocol
operates between a management station, acting as the control
center for network monitoring, and an agent, the network
device that is being managed by the management station. The
management station will send out requests to the agent for
data on configuration, operational status, and performance
statistics. SNMP uses five control primitives or commands
to monitor a network device: GetRequest/Set Request,
GetResponse, GetNextRequest, and Trap. GetRequest,
GetNextRequest, and SetRequest initiate data flows from the
management station to an agent on the network. The agent
will respond with GetReponse to any of these primitives.

The agent, however, can also send an uninitiated primitive to the management station using the Trap primitive to alert the station of an unusual event that may need attention.

It is important to remember that SNMP agents cannot perform any analysis on the information they collect, they can only send out a Trap primitive and alert the management station that they have information to give it. The management station will then aggregate the data it receives back from its agents. The burden of actually analyzing and drawing conclusions from the information provided to the management station is the responsibility of the administrator responsible for the management station. In some cases, multiple management stations can be run on the same network and their aggregate data can be sent to a central location for analysis.

There are three versions of SNMP in use today - SNMPv1, SNMPv2, and SNMPv3. The second version of SNMP introduced new management capabilities including: manager-to-manager communication to allow multiple station managers to be running on the same network, enhanced security, and improved efficiency and performance. The testing that was carried out by Oulu University Secure Programming Group (OUSPG) that revealed the vulnerabilities in the protocol was only performed on SNMPv1. It is believed that similar vulnerabilities may exist in the later versions of SNMP.

Vulnerabilities

Recently, a lot of press has been given to the vulnerabilities the Oulu University Secure Programming Group (OUSPG) has found in SNMPv1 implementations. But long before these vulnerabilities were discovered another vulnerability existed that can have just as much impact on an organization's systems as the two new vulnerabilities brought to light by OUSPG. According to Deborah Radcliff, "SNMP uses the community name 'default'… if this community name isn't changed, attackers can slip right in and control SNMP to map your network, change routes of packets and all kinds of evil things." (www.computerworld.com - "Cover you SNMP") She goes on to say that attackers could even change IP addresses and bring down critical interfaces. This

vulnerability has been public for over two years, but it still warrants attention because of the amount of network exposure that could result if this vulnerability were exploited.

A community string or community name is a weak form of authentication used by SNMP agents and management stations. An agent can be configured as read-only, read-write, or no access based on the community string used in the packets sent to an agent from the management station. Changing the community string from "default" to another identifier will help to mitigate the risks presented by this vulnerability. However, the community string is not encrypted in the packets that are sent to the agents, instead the community string is sent in plain-text, leaving it open to possible packet sniffing by would-be attackers. Even with the community string changed, this method of authentication should not be relied upon to secure the protocol. This method should be used in conjunction with other security measures to thoroughly mitigate these risks.

The potential impacts of this vulnerability are large and far-reaching. Once an attacker has access to the SNMP, they can not only see all the hardware that is running on the system, but also the information that is being exchanged through the network. The attacker can also see UDP services that could reveal the other active network services that an organization is running on their network. This vulnerability also opens systems up to additional vulnerabilities. If an attacker can map the network they can target critical services and devices running on the system for other attacks. Critical machines such as Domain Name Servers and Mail Servers can easily be found if an attacker is able to map the network. These two machines are a favorite of attackers who want to gain access to password files. Once an attacker gains access to a password file the network can be opened up further.

The most recent vulnerabilities in SNMP that were discovered by OUSPG may also have heavy impacts on systems. According to CERT Advisory CA-2002-03 the two new vulnerabilities discovered are:

VU#107186–Multiple vulnerabilities in SNMPv1 trap handling:

> "SNMP trap messages are sent from agents to
> managers. A trap message may indicate a warning or
> error condition or otherwise notify the manager
> about the agent's state. SNMP managers must
> properly decode trap messages and process the
> resulting data. In testing, OUSPG found multiple
> vulnerabilities in the way many SNMP managers
> decode and process SNMP trap messages."
> (www.cert.org - CERT Advisory CA-2002-03)

VU#854306-Multiple vulnerabilities in SNMPv1 request
handling:

> "SNMP request messages are sent from managers to
> agents. Request messages might be issued to obtain
> information from an agent or to instruct the agent
> to configure the host device. SNMP agents must
> properly decode request messages and process the
> resulting data. In testing, OUSPG found multiple
> vulnerabilities in the way many SNMP agents decode
> and process SNMP request messages." (www.cert.org -
> CERT Advisory CA-2002-03)

OUSPG initiated a two-pronged test that would send thousands
of malformed SNMPv1 packets to an agent. The first part of
the test focused on the get, getnext, and set operations of
SNMP, while the second part of the test generated traps.
SNMP products by all vendors tested failed these tests,
exposing the vulnerabilities in SNMP.

These vulnerabilities are caused by differences in the ways
vendors' devices receive, decode, and process SNMP service
requests. If SNMP packets are malformed, errors in
processing can occur either at the agent or at the
management station. Depending on the device or vendor, these
processing errors can cause a device to reboot or crash.

The potential impacts from these vulnerabilities can range
from denial-of-service conditions, format string
vulnerabilities, and buffer overflows. According to CERT,
attackers may even be able to gain unauthorized access to

systems.   The impact of these vulnerabilities will not only
affect a network, but could have far-reaching business
impacts on a company's bottom line.   For a business that has
built their business model around e-commerce, a denial-of-
service attack that brings down their site could be
extremely costly.   Likewise, if an attacker gained
unauthorized access to a network, passwords could be
harvested, possibly giving the attacker access to extremely
confidential information such as customer credit card
numbers or employee benefit information.   The potential
business impacts of an attack like this could also cost a
company dearly either in the form of lost revenue or
degradation of reputation.

One thing that makes these vulnerabilities so critical is
the fact that the use of SNMP is so ubiquitous in the world
of network management.   With so many networks at risk
because of these vulnerabilities, it is necessary to address
these issues quickly.   The fact that these vulnerabilities
have been made public is helpful to administrators trying to
keep their networks secure; on the other hand, it also makes
everyone a potential target because would-be attackers are
now aware of the vulnerabilities as well.   Patching these
vulnerabilities is not an option if one wants their network
to be secure, either patch the devices or shut off the
service.

Major Vendors Affected

As it turns out, one of SNMP's early features that was
heralded as one of its greatest strengths, may now turn out
to be one of its greatest weaknesses.   The simplicity of
this protocol has allowed for widespread use and
interoperability across systems, unfortunately, this now
also leaves most networks vulnerable and has most vendors
clamoring for fixes.   SNMP usage is not limited to what most
people think of as typical network devices, like routers.
SNMP runs on operating systems, cable and DSL modems, image
scanners and digital cameras, printers, copiers and fax
machines, network management devices, and many other devices
not typically thought of as core network devices.   Cisco,
Sun, and Microsoft are just a few of the major vendors whose
products are affected by these newly discovered

vulnerabilities.

Cisco, a major producer of network routers and hubs, has a number of devices that are susceptible to these vulnerabilities if they are exploited. Typically, if exploited, these vulnerabilities would cause the Cisco device to crash and reboot. An attacker could carry out a denial of service attack by flooding a network with malformed SNMP messages that cause the network devices to crash once they try to process the SNMP requests. Cisco has attempted to generate fixes for all of its products that are susceptible to these vulnerabilities; however not all of their products have fixes yet. Cisco recommends that their customers go to the Cisco website to check for fixes and upgrade the release of their hardware to patch these vulnerabilities, if patches exist. (www.Cisco.com)

Sun Microsystems, a major producer of core network devices and servers, is another major vendor that has been affected by these recent vulnerabilities. According to Sun's security bulletin, Sun's Solstice Enterprise Master Agent - snmpdx, is vulnerable to a buffer overflow that, if exploited, would allow root access to the affected system. Root access to a network would give a potential attacker most of the information they need to take full advantage of a network and the information contained within it. Like Cisco, Sun has quickly found ways to patch their systems and have made these patches available on their website. (www.sun.com)

Even Microsoft products have been affected by these vulnerabilities. Like Cisco and Sun, exploiting these vulnerabilities will cause a buffer overrun, which could result in a denial of service. Both Microsoft Windows 2000 and the Windows XP operating systems are susceptible to these exploits, as they provide for SNMP implementation. One positive in this case, however, is that SNMP implementation is not part of the default installation for either operating system. This helps to minimize the risk that users are running systems with vulnerabilities they don't know they are susceptible to. Similar to the other two vendors we have looked at, Microsoft is also developing patches for their systems to eliminate the vulnerability.

The Microsoft website has full details on patches that have
and are being developed. The first step in patching the
vulnerabilities affecting either Windows version is to check
to see if the SNMP service has been enabled. If the SNMP
service is not installed on the operating system, the
operating system is not vulnerable, although other devices
running on the network may still be vulnerable.

Unilaterally, vendors and watch groups alike are
recommending network administrators disable all of their
SNMP services as a near-term fix until all of the
vulnerabilities in the system can be adequately patched.
One of the difficulties faced by network administrators now
is the widespread need for patches throughout their
networks. As Josh Turiel, the network services manager at
Holyoke insurance company, said, "The more intricate your
network is, the more exposed you are."
(www.computerworld.com - "SNMP Devices Open to Attacks"
Again, the interoperability of this protocol has made almost
everything from routers to operating systems vulnerable to
these threats, making the job of patching a system quite a
headache for administrators. Literally every layer of the
network will need to be thoroughly checked for potential
vulnerabilities. Once discovered, these holes will need to
be patched if fixes are available. If fixes aren't
available for some of the products on the network running
SNMP, an interim workaround solution will need to be
developed until everything can be patched.

Solutions and Alternatives

While these vulnerabilities do pose serious risks to
networks operating SNMP, the risks they expose an
organization to can be mitigated in a number of ways. The
obvious first step in this process would be to disable all
SNMP services. Disabling SNMP services will eliminate any
risks associated with these vulnerabilities, as SNMP has to
be running for the vulnerabilities to be exploited. Still,
SNMP provides a valuable service to network administrators
so most businesses will consider this step only a short-term
fix. Disabling SNMP services will allow system
administrators time to check the devices running on their
networks so that vendors can be contacted regarding fixes

and patches.

Patches and fixes are another avenue that can be used to
mitigate the risk associated with these vulnerabilities.
While patches and fixes may eliminate the vulnerability in a
certain device, they can only mitigate the risk to a network
if the patches are installed! So, the identification of
vulnerable devices and the subsequent installation of
patches on affected devices will help to mitigate these
risks.

In addition to patching vulnerable devices, ingress and
egress filtering can be performed on the network. Ingress
filtering filters network traffic as it enters the network
and egress filtering filters network traffic as it leaves
the network. Only those devices that have a business need
to accept inbound traffic should do so. Likewise, only
devices that have a business need to initiate outbound
traffic should do so. Extraneous inbound or outbound
communication could indicate an attack is being initiated on
the network. Monitoring outbound traffic is a powerful
diagnostic to prevent your network from being used to attack
another unsuspecting networks with similar vulnerabilities.
The presence of unusual amounts of outbound traffic could
indicate the network is being used in the attack of another
network. If unusual outbound traffic is caught in time,
disabling the system could help prevent or cut-short another
attack on a similar network.   Ports 161 and 162 both
provide SNMP services; these ports should be filtered and
watched closely.

Another type of filtering can be performed to help mitigate
risk as well. SNMP packets can be filtered to determine
what devices are sending them. Agents should only accept
traffic that comes from known management stations and
management stations should only accept traffic that is
responding to a valid request or a trap sent from a known
agent. For example, SNMP traffic from a management stations
should come from inside the network. If the filter detects
that this traffic is coming from an external source it
should alert the system. This security measure will help to
ensure that an attacker is not spoofing SNMP traffic to gain
access or shut down the network.

Another way to keep an eye on a network is to log traffic coming into, flowing through, and exiting the network. Logging is by no means a security strategy specific to these SNMP vulnerabilities; it is a generally accepted best practice to help secure systems. Traffic logging can help network administrators notice unusual traffic patterns that may indicate an attack. Logging will not prevent the attacks, but it can help network administrators gain valuable information regarding who is attacking them and what methods they are using.

As mentioned above, a specific fix to address the community string vulnerability is relatively simple to implement, change the default community strings. This does not, however, guarantee that an attacker will not gain access to a network using this vulnerability. The community string can still be cracked if an attacker intercepts a packet with the community string in it. This will, however, make the attacker work harder and longer to crack the community string, possibly giving a security administrator enough time to detect the potential attack and react to it.

Conclusion

Vendors and watch groups alike have done a great job of educating the public on these vulnerabilities and working to find solutions and patches to these problems so that SNMP can be implemented and used without fear of repercussions. Still, all the patches and public knowledge cannot take the place of an organized, well secured network. The burden of eliminating vulnerability ultimately falls squarely on the shoulders of network administrators and security administrators who need to be proactive in installing patches and vigilant about monitoring their systems.

Securing systems goes way beyond installing the appropriate patches to fix system vulnerabilities, although this is a good place to start. A combination of techniques should be used to thoroughly secure systems. The use of firewalls, vulnerability scanners, virus protection and a combination of host based intrusion detection and network intrusion detection systems will help to mitigate the risk of a system

compromise that could have dangerous impacts on a business.
The introduction of these new SNMP vulnerabilities proves
that the security landscape of a network is always changing.
Flexibility is a crucial mindset for a network administrator
to possess when it comes to security. Just because
vulnerabilities have been found in the SNMP protocol, does
not mean it needs to be abandoned as a means of network
management. Appropriate precautions should be taken to
mitigate the risks it presents. As with most things that
are valuable to a company, a certain amount of risk must be
accepted to reap the benefits of the returns it affords the
business.

SNMP is a valuable protocol that enables network
administrators to effectively manage their network. SNMP
strengths lie in its low overhead and high interoperability
among network devices, operating systems, and other
peripherals. The risks and impacts of these vulnerabilities
have been augmented by the depth and breadth of SNMP's use
in the market, an affect of its interoperability. I guess
it is true what they say; your greatest strength can become
your greatest weakness.

Works Cited:

CERT Advisory CA-2002-03. "Multiple Vulnerabilities in Many Implementations of Simple Networking Management Protocol." http://www.cert.org/advisories/CA-2002-03.html

Cisco Security Advisory: "Malformed SNMP Message-Handling Vulnerabilities" http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

Connected: An Internet Encyclopedia. "SNMP Protocol Overview" http://freesoft.org/CIE/Topics/108.htm

Carnegie Mellon University. "Simple Network Management Protocol" http://www.sei.cmu.edu/str/descriptions/snmp_body.html

Dean, Joshua. "Newly Identified Security Gaps Threaten Internet." http://www.govexec.com/dailyfed/0202/021502j1.htm

Microsoft Security Bulletin. "MS02-006" http://www.microsoft.com/technet/security/bulletin/NS02-006.asp?frame=true

Radcliff, Deborah. "Cover Your SNMP." http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO41144-,00.html

SNMP Research International, INC. "SNMP Research: CERT/OUSPG Update" http://www.snmp.com/cert.html

Sun Security Bulletins. "Article 215" http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=col&doc=secbull/215&type=0&nav=sec.sba

Vijayan, Jaikumar. "SNMP Devices Open to Attacks." http://www.computerworld.cwi/Printer_Friendly_version/0,1212,KEY73_STO68438-,00.html