Outpost24

Vulnerability Management made easy

SNMP Scanning

Configuration Guide

Version: 1.1

2018-12-18

Table of Contents

About This Document

This document elaborates on the requirements of authenticated SNMP scanning.

For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

1 Introduction

This document elaborates on the requirements of authenticated SNMP scanning.

To support authenticated SNMP support where net-snmp does not allow access to epoch of RPM database, a custom script is needed.

SNMP v1 and v2c is unencrypted, so values (including community names) from queries and responses sent to and from the SNMP-monitored device can be read by someone with access to the network.

SNMP v3 and v2c both provide the same data and although v3 has a slight performance overhead because it encrypts the traffic. The ease of management of using the same protocol across the network makes a very strong case for using only SNMP v3.

Caution!

SNMP should be considered as sensitive data so this should only be allowed on trusted networks and using SNMP v3 since SNMP v1 and v2 is unencrypted.

2 Requirements

Only the following distributions are handled by this script:

- RHEL
- CentOS

3 Script

Caution!

It is important to limit the write access to this script, as it will run as root every time a request is made. Also note that its path is obtainable over SNMP.

```
#!/bin/sh
distro=$(grep -Eo '^ID=\"[A-Za-z\.]+\"' /etc/os-release \
2>/dev/null)
if [ $? -ne 0 ]
then
    distro="unknown"
else
    distro=`echo $distro | sed 's/ID=\"\(.*\)\"/\1/g'`
fi
echo $distro
/bin/rpm -qa -qf \
'%{NAME}|%{EPOCH}:%{VERSION}|%{RELEASE}|%{SOURCERPM}\n'
exit $?
```

4 Configuration

To make this script available over SNMP:

1. Copy the script in section 3 and save it as `/etc/snmp/o24-rpm.sh`.
2. Make the script write protected and executable.

```
# chmod a-w,o+x /etc/snmp/o24-rpm.sh
```

3. Edit the `/etc/snmp/snmpd.conf` file and add the extend directive by enter the following:

```
extend o24-rpm-db /etc/snmp/o24-rpm.sh
```

4. Restart the SNMP daemon:

```
$ sudo service snmpd restart
```

5. To verify that everything is working, perform the `snmpwalk` command as shown in the example below:

```
snmpwalk -v 3 -a MD5 -x DES -u 'user' -A 'pass' -X 'pass' \
-l authPriv
localhost \
.1.3.6.1.4.1.8072.1.3.2.4.1.2.10.111.50.52.45.114.112.109.45.
100.98
```

Which translate into:

```
NET-SNMP-EXTEND-MIB::nsExtendOutLine."o24-rpm-db"
```