

Re: snmp vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-07/0006.html>

From: H Carvey (keydet89@yahoo.com)

Date: 07/19/01

Date: 19 Jul 2001 17:08:17 -0000
Message-ID: <20010719170817.256.qmail@securityfocus.com>
From: H Carvey <keydet89@yahoo.com>
To: pen-test@securityfocus.com
Subject: Re: snmp vulnerabilities

> *As for comments on protecting SNMPv1 with ACL's and obfuscated Community Strings, that is laughable at best. A better solution is to run with SNMPv3 using AuthPriv functionality, seems like some of the popular management systems don't yet support v3 capabilities.*

Well, I don't see why such a solution would be laughable. From a business perspective, it doesn't necessarily make sense to keep heaping layer after layer of 'stuff' on top of the protocol.

Oddly enough, my post about treating SNMP in isolation was rejected by the moderators, who as yet have not responded to my queries regarding this issue.

The issue as I see it is that folks are treating security mechanism in general (SNMP is not a security mechanism) in isolation. Yes, an obfuscated community string in the UDP packets is laughable in the face of a simple sniffer. However, if your infrastructure configuration allows for the undetected installation of a sniffer, then you have more things to be concerned with, other than simply the 'safety' of your community strings. If someone has a sniffer, why bother with things like community strings at all, when the admin passwords can be easily collected.

SecurityFocus Penetration: Re: snmp vulnerabilities

Properly configuring and monitoring your entire infrastructure is what can allow things like SNMP and TFTP to run on the network. Network engineers too often say that "security breaks stuff"...and they are definitely correct, particularly when a security 'expert' doesn't keep the business objectives in mind.

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- ***Previous message:*** Gary Warner: "HP3000"
- ***Next in thread:*** Dom De Vitto: "RE: snmp vulnerabilities"
- ***Reply:*** Dom De Vitto: "RE: snmp vulnerabilities"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]