OpenVAS

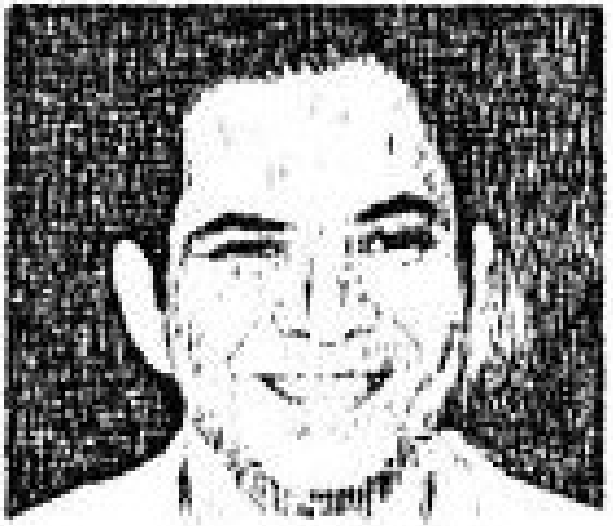
Open Vulnerability Assessment System

Mauro Risonho de Paula Assumpção
Security Researcher
OpenVAS Project

GTS Grupo de Trabalho em Segurança

http://gts.nic.br/reunioes/gts-22/

In memorian



Alberto Fabiano Medeiros

in

br.linkedin.com/in/albertofabiano

Who i am?

- **Entusiasta em segurança**
- **Security Researcher OpenVAS Project** www.openvas.org (desenvolvedor de plugins OpenVAS)
- **Moderador/Tradutor/Colaborador do Backtrack Linux** www.backtrack-linux.org
- **Fundador do Backtrack Brasil** – Site não oficial (2008-2012) www.backtrack.com.br (não tenho nada a ver com a equipe atual).
- **Palestrante na OWASP** www.owasp.org e ZapEvangelist do Zaproxy https://code.google.com/p/zaproxy/wiki/ZapEvangelists

Who i am?

- **Pesquisador OWASP OWTF** (Offensive (Web) Testing Framework, is an OWASP+PTES-focused)
- **Pesquisador PTES** (http://www.pentest-standard.org/) (aguardando ser adicionado ao projeto)
- Entusiasta da linguagem **Golang** ww.golang.org (do Google)
- Pesquisador em segurança e Autodidata em geral.
- Nerd estilo década de 80 e minha esposa é “pin-up” estilo “geek”:)
- Um cara persistente em seus objetivos e metas e tem muito que aprender ainda...
- Sou “Risonho” e isso é obvio, vejam meu sobrenome !:)

SONHO DE CONSUMO PROFISSIONAL ATUALMENTE

TRABALHAR
FULL TIME
EM
R&D

OpenVAS

- OpenVas começou GNessUs, como um fork do Nessus, que era open source (GPL2) da Tenable Network Security e se tornou proprietário em outubro de 2005.

- OpenVAS foi originalmente modificado por pentesters no Portcullis Security, liderado por Tim Brown.

Estatísticas

Ohloh BY BLACK DUCK

https://www.ohloh.net/p?q=openvas

OpenVAS

Compare

Analyzed 5 days ago

OpenVAS is an open source remote security vulnerability scanner, designed to search for networked devices and computers, discover accessible ports and services, and to test for vulnerabilities on any such ports; plugins allow for further expansion.

245K	lines of code
18	current contributors
5 days	since last commit
14	users on Ohloh

Very High Activity

1 Review

Mostly written in C

Licenses: GPL-2.0+

network security vulnerability scanner

openvas-plugins

Compare

Analyzed about 1 month ago

Network vulnerability tests collection for OpenVAS.

79	lines of code
11	current contributors
About 1 month	since last commit
2	users on Ohloh

Activity Not Available

0 Reviews

Mostly written in shell script

Licenses: GPL-2.0+

vulnerability network security scanner

Citações Internacionais

MITRE CVE OVAL Celebrating 10 Years

http://oval.mitre.org/adoption/participants.html#OpenVAS

OpenVAS

Date Declared: July 6, 2012

Web Site: www.openvas.org

Quote/Declaration: OpenVAS is a vulnerability management and vulnerability scanning software framework. A feed service allows regular updates of Network Vulnerability tests (NVTs). The main security scan phase of the application collects security information about each host in the network being scanned. Subsequently, comprehensive OVAL-related processing is possible. his includes exporting system characteristics for the whole network, and applying the applications reporting framework according to OVAL Definitions.

PRODUCT NAME: OpenVAS

Type: Vulnerability Management

OVAL ADOPTER oval.mitre.org

OVAL Authoring Tool: *No*
OVAL Definition Evaluator: *Planned*
OVAL Definition Repository: *No*
OVAL Results Consumer: *Planned*
OVAL System Characteristics Producer: *Yes*

Review Completed Questionnaire

Citações Internacionais

- http://iac.dtic.mil/csiac/download/vulnerability_assessment.pdf

IATAC

http://iac.dtic.mil

Open Vulnerability Assessment System 4

Abstract

The Open Vulnerability Assessment System (OpenVAS) is a framework of several custom-built and third-party services and tools that collectively implement a vulnerability scanning and vulnerability management solution. The included security scanner is updated daily through a feed of Network Vulnerability Tests; as of January 2011, the scanner supported 20,000 different vulnerability tests. OpenVAS Scanner can scan many target hosts concurrently, and can perform tests *via* an SSL session connection if necessary. OpenVAS Manager can manage multiple OpenVAS Scanners concurrently. It also provides management of scan results, including false positive verification and reduction, and scan operation (start, pause, stop, resume, scheduling). It also provides reporting capabilities, *via* plug-ins, in multiple formats, including (but not limited to) XML, HTML, and LaTeX. The OpenVAS Administrator enables configuration of the OpenVAS user accounts, and synchronization of its data feeds. All OpenVAS tools are accessible *via* Greenbone clients—either a remote client (that can be run from a thin/lean client with only a browser), a full desktop client

Open Vulnerability Assessment System 4

Type	Multilevel Scanner
Target(s)	Networks, Web applications
Format	Software, Appliance, or SaaS
OS	Linux (CentOS/Fedora/Red Hat/Debian/ OpenSuSE/Ubuntu/Scientific Linux/ Mandriva/Gentoo®/Slackware/SuSE Linux Enterprise/ArchLinux/BackTrack); FreeBSD; Windows
Hardware	
License	Open source
SCAP Validated	
Standards	
Supplier	Atomic Corporation's OpenVAS Project (Germany)
Information	*http://www0.atomicorp.com/index.html*

Citações Internacionais

http://www.dfn-cert.de/en.html

Citações Internacionais

https://www.bsi.bund.de/DE/Home/home_node.html

Arquitetura

- The Open Vulnerability Assessment System (OpenVAS) é um framework vários serviços e ferramentas.
- http://www.openvas.org/integrated-tools.html

arachni
web application security scanner framework

NMAP

OpenLDAP™
http://www.OpenLDAP.org

SNMPWALK

The Hacker's Choice

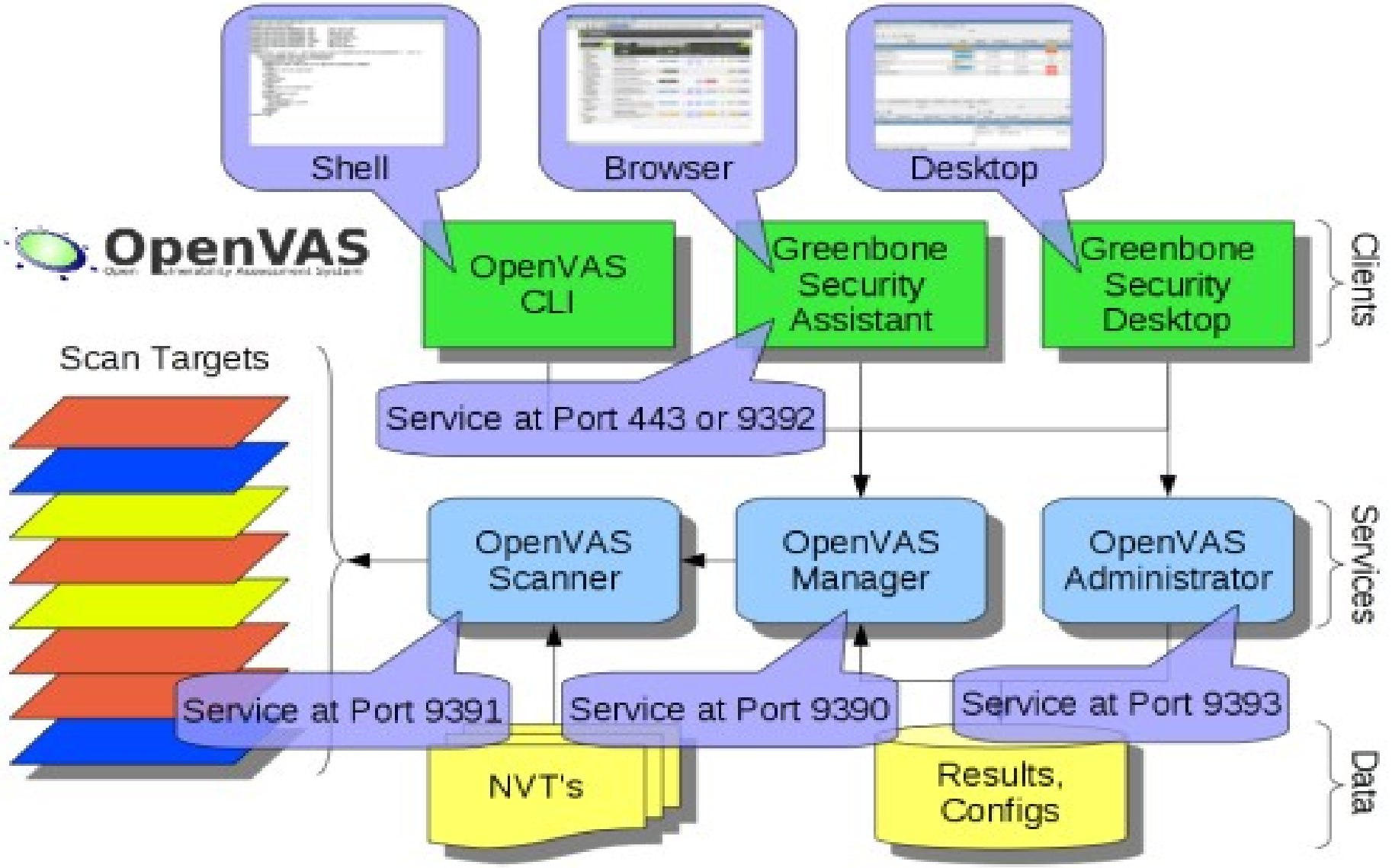
NTA

SNORT™

w3af
Web Application Attack and Audit Framework

chkrootkit

Arquitetura

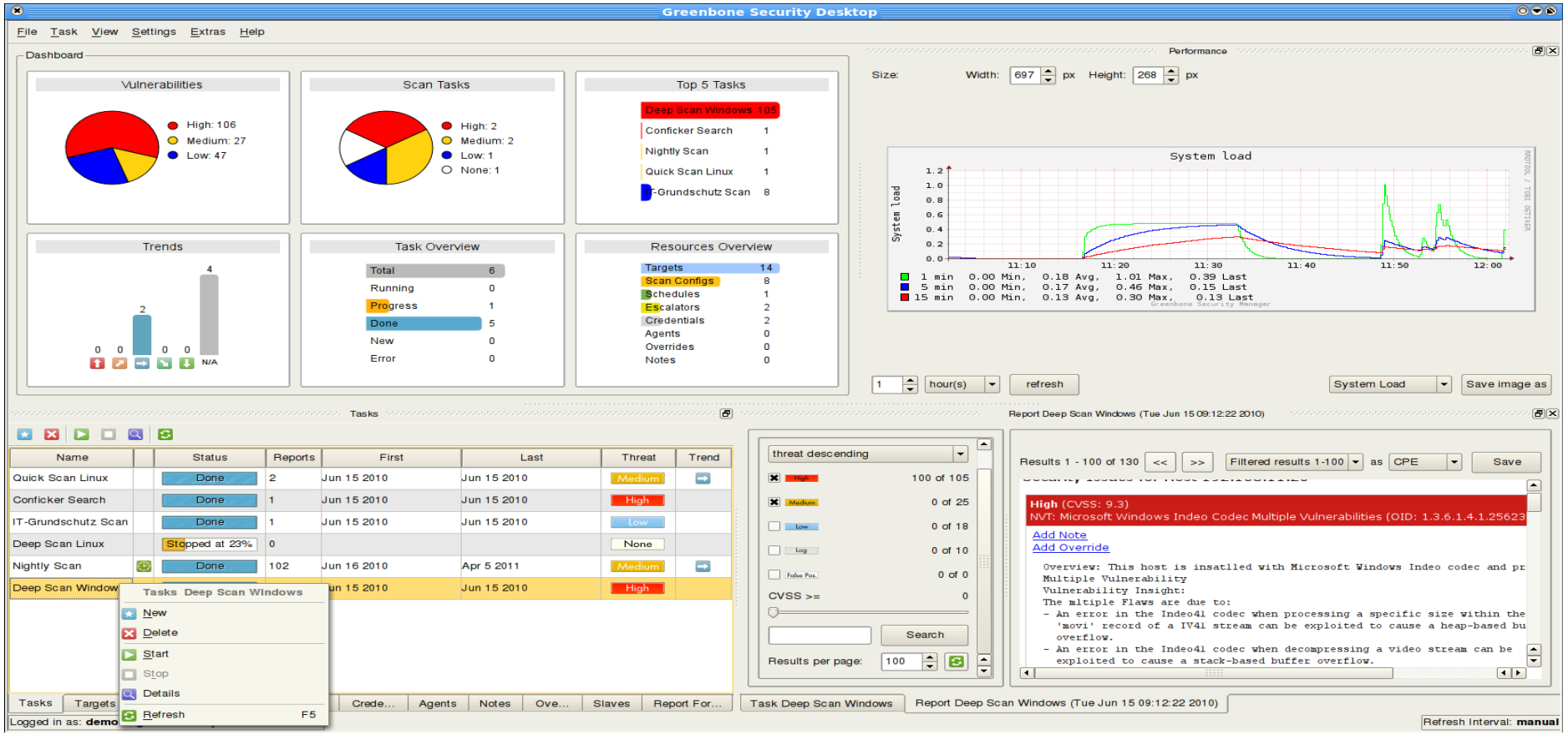


OpenVAS Manager

- The OpenVAS Manager é o serviço/gerenciador central que consolida as varreduras de vulnerabilidades e outras informações importantes durante o(s) scanning(s).

Greenbone Security Desktop (GSD)

- Greenbone Security Desktop (GSD) cliente desktop feito em Qt e que executa o protocolo OMP



OpenVAS Scanner

- The OpenVAS Scanner é o serviço/gerenciador central que consolida as varreduras de vulnerabilidades e outras informações importantes durante o(s) scanning(s).

OpenVAS CLI

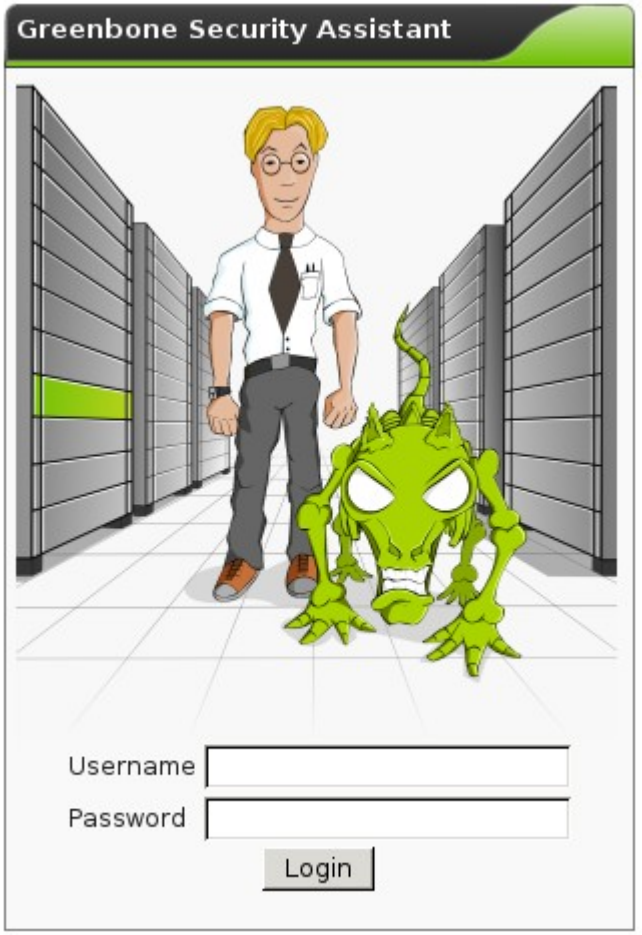
- OpenVAS CLI contém a ferramenta de linha de comando"omp" que permite criar processos batch para serem executados no OpenVAS Manager.

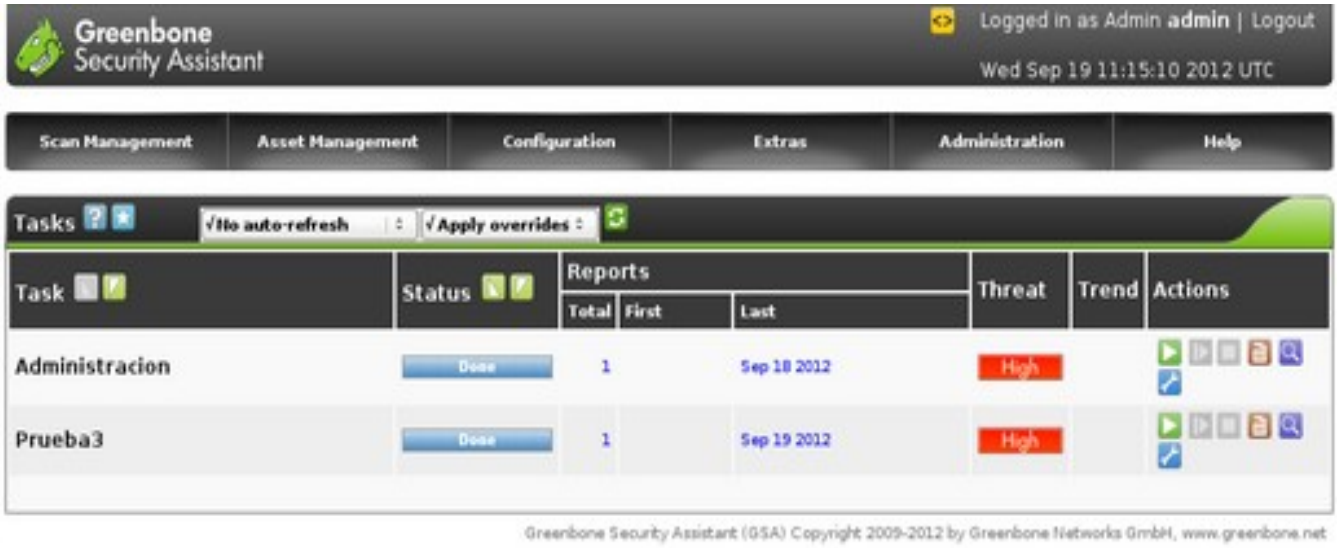
OpenVAS Administrator

- OpenVAS Administrator atua como uma ferramenta de linha de comando ou como um daemon de serviço que oferece o OpenVAS Administration Protocol (OAP). Este serviço é mais focado em Controle de acesso e administração de usuários que vão utilizar o OpenVAS

GSAD – Greenbone Security Assistent

- GSAD uma interface gráfica web, que atua para administração do OMP via web.





OpenVAS Administrator

- OpenVAS Administrator atua como uma ferramenta de linha de comando ou como um daemon de serviço que oferece o OpenVAS Administration Protocol (OAP).

- Este serviço é mais focado em Controle de acesso e administração de usuários que vão utilizar o OpenVAS

PLATAFORMAS/SERVERS DEPLOYMENT

http://www.openvas.org/install-packages.html

Plugins NASL by firebits

- https://github.com/firebitsbr/OpenVAS-Plugins-hardening/tree/master/plugins
- svn checkout https://scm.wald.intevation.org/svn/openvas-nvts

```
33
34  Vulnerability Insight:
35
36  CVE-2010-0547 samba: mount.cifs improper device name and mountpoint
37  strings sanitization
38  The MITRE CVE dictionary describes this issue as:
39
40  client/mount.cifs.c in mount.cifs in smbfs in Samba 3.4.5 and earlier
41  does not verify that the (1) device name and (2) mountpoint strings are
42  composed of valid characters, which allows local users to cause a
43  denial of service (mtab corruption) via a crafted string.
44
45  Affected Software/OS:
46  cifs on Red Hat Enterprise Linux version 4 (samba)
47
48  Fix: Please Install the Updated Packages.
49
50  References:
51
52  https://access.redhat.com/security/cve/CVE-2010-0547
53
54  http://rpmfind.net/linux/rpm2html/search.php?query=samba&#8221;;
55
56  if(description)
57  {
58  script_id(880323);
59  script_version("$Revision: 12798 $");
60  script_tag(name:"check_type", value:"authenticated package test");
61  script_tag(name:"last_modification", value:"$Date: 2013-07-11 18:03:54 GMT-03:00 0 Brazil, São Paulo (Thu, 11 Jul 2013) $");
62  script_tag(name:"creation_date", value:"2009-02-27 08:31:09 +0100 (Fri, 27 Feb 2009)");
63  script_tag(name:"cvss_base", value:"2.6");
64  script_tag(name:"cvss_base_vector", value:"AV:N/AC:L/Au:N/C:N/I:N/A:P");
65  script_tag(name:"risk_factor", value:"Low");
```

DEMO

PERGUNTAS ?

mauro.risonho@gmail.com

http://br.linkedin.com/pub/mauro-risonho-de-paula-assump%C3%A7%C3%A3o/b/b06/225/

http://twitter/firebitsbr

http://firebitsbr.wordpress.com/

OBRIGADO
PELA
OPORTUNIDADE !

mauro.risonho@gmail.com

http://br.linkedin.com/pub/mauro-risonho-de-paula-assump%C3%A7%C3%A3o/b/b06/225/

http://twitter/firebitsbr

http://firebitsbr.wordpress.com/