Pakiti – Patching Status System

Michal Procházka

OSCT F2F Meeting - Amsterdam

History

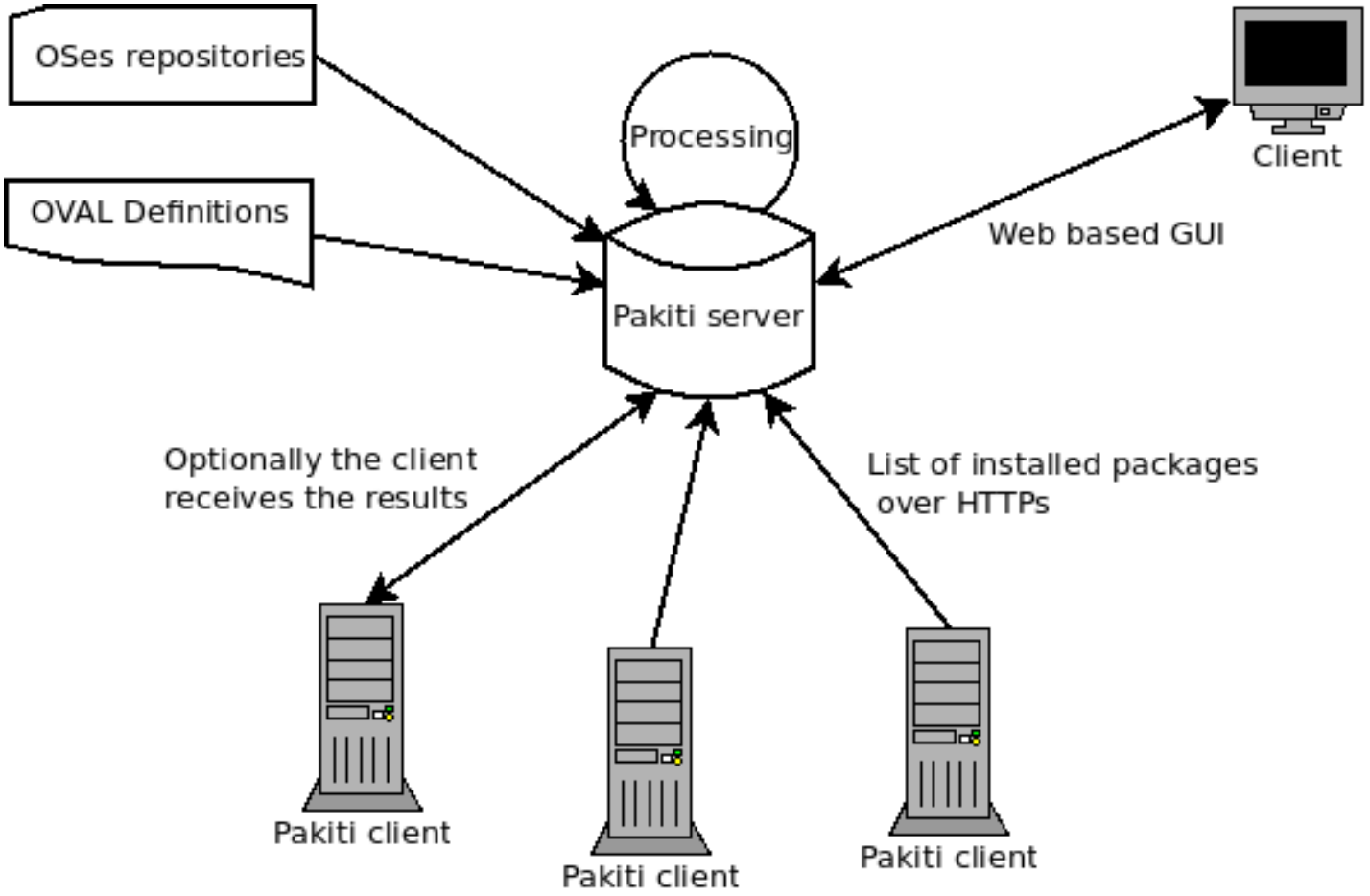
- **Yumit**
  - Written by Steve Traylen (RAL)
  - Client has to have root privileges
- **Pakiti v1.0**
  - Improved Yumit by Romain Wartel
- **Pakiti v2.0**
  - Re-scoped the tool to focus on security patches
  - Support for OVAL data
  - Client does not need root privileges
- **Pakiti v2.1**
  - Current version
- **Future: Pakiti v3.0**

Pakiti v2.1 Overview

- **Provides information about**
  - Installed packages and theirs versions on the monitored hosts
  - If the installed packages are up to date
  - List of vulnerabilities of the concrete package version
  - Package that represents currently running kernel

Vulnerabilities Definition Sources

- **OS Repositories**
  - Each Linux OS vendor maintains package repositories
  - It contains the most recent version of the packages
  - Some are distinguished as security, updates, extra repositories
- **OVAL Definitions**
  - Language using XML for describing the conditions, when a vulnerability (CVE) is applicable on the host system
  - RedHat, SuSE, Sun Solaris currently publishes OVAL
  - Format is not identical across different OS vendors
  - More info at http://oval.mitre.org


OSes repositories
OVAL Definitions
Processing
Pakiti server
Client
Web based GUI
Optionally the client
receives the results
List of installed packages
over HTTPs
Pakiti client
Pakiti client
Pakiti client

Server internals

- Server receives the list of installed packages from the host
- Checks whether the host reporting right hostname (based on IP)
- Stores list of installed packages in the DB
  - Do not store *-doc, *-dev/devel and user selected packages
- If asynchronous mode is disabled, then checks each package during reporting, if it is up to date
- If the client requests reporting, then the list of outdated packages is sent back to the client

- In asynchronous mode, packages are checked using script recalculate_vulnerabilities.php (can be run by the cron)
- The script recalculates only affected hosts

Server Capabilities

- Support for Oses using dpkg and rpm (APT, RPM repositories)
- Checks hosts packages against OS vendor repositories
- Checks RH based system against RH OVAL definitions
- Selects package, that represents running kernel
- Shows when the host reported for the last time
- Compute statistics for the host and domain
- Uses dpkg and rpm cmp function ported to the PHP
- Grouping hosts by the domain, TLD and tag
- Searching hosts by installed package
- Searching hosts by concrete CVE
- Anonymous view on the concrete domain results

Pakiti Client

- **Simple bash script**
- **Transfers data over HTTPs**
  - Openssl or Curl can be used
- **Can be run in various ways**
  - Crontab job
  - Nagios/SAM probe
- **Bash script is configurable**
  - Build-in configuration
  - Or separate configuration file /etc/pakiti2/pakiti2-client.conf

Pakiti Client Configuration

```
servers_name = pakiti.server.com:443 pakiti2.server.com:8443
# CA Path, where is located certificate of the CA which issued SSL
    certificate for the Pakiti server
ca_certificate = /etc/grid-security/certificates
# The client certificate and the key
#host_cert = /etc/ssl/host.pem
# Connection method: 'curl' or 'openssl' (default) or 'stdout'
connection_method = openssl
openssl_path = /usr/bin/openssl
#curl_path = /usr/bin/curl
# Put something small that can identify your site/host/team, without
    spaces.
tag = TEST
# Does the client should report back the list of packages needs upgrade?#
    (default 0 - off)
report = 1
```

Pakiti Server Configuration

- **Interesting options**
  - store_devel_packages
  - store_doc_packages
  - ignore_packages_list
  - anonymous_links
  - anonymous_link_lifetime
  - ext_pages_outdated
  - asynchronous_mode

Production

- **Pakiti v2.1 runs on the EGEE**
  - https://pakiti.cern.ch (restricted access)
  - Currently monitors around 1200 hosts per day
  - The test is executed by the SAM probe
  - Hosts are purged every day, because SAM probes land on a different hosts of the sites
  - Before the hosts are purged, the backup is made
  - Server runs in synchronous mode, the processing of one host takes from 0,5s to 12s, depends on the number of hosts, which reporting at the same time
  - It provides only representative sample, we assume that the clusters are homogeneous, which isn't always true
  - Christos tested successfully Nagios probes

Other Installations

- **MetaCentrum – Czech National Grid Infrastructure**
  - Approximately 1000 hosts are monitored
- **Fermilab**
  - Approximately 1900 hosts are monitored
- **Department of Particle Physics, University of Oxford**
  - Using Pakiti 1.0.1 – 140 hosts
  - Currently migrating to the Pakiti 2.1
- **OSG, FZK, ...**

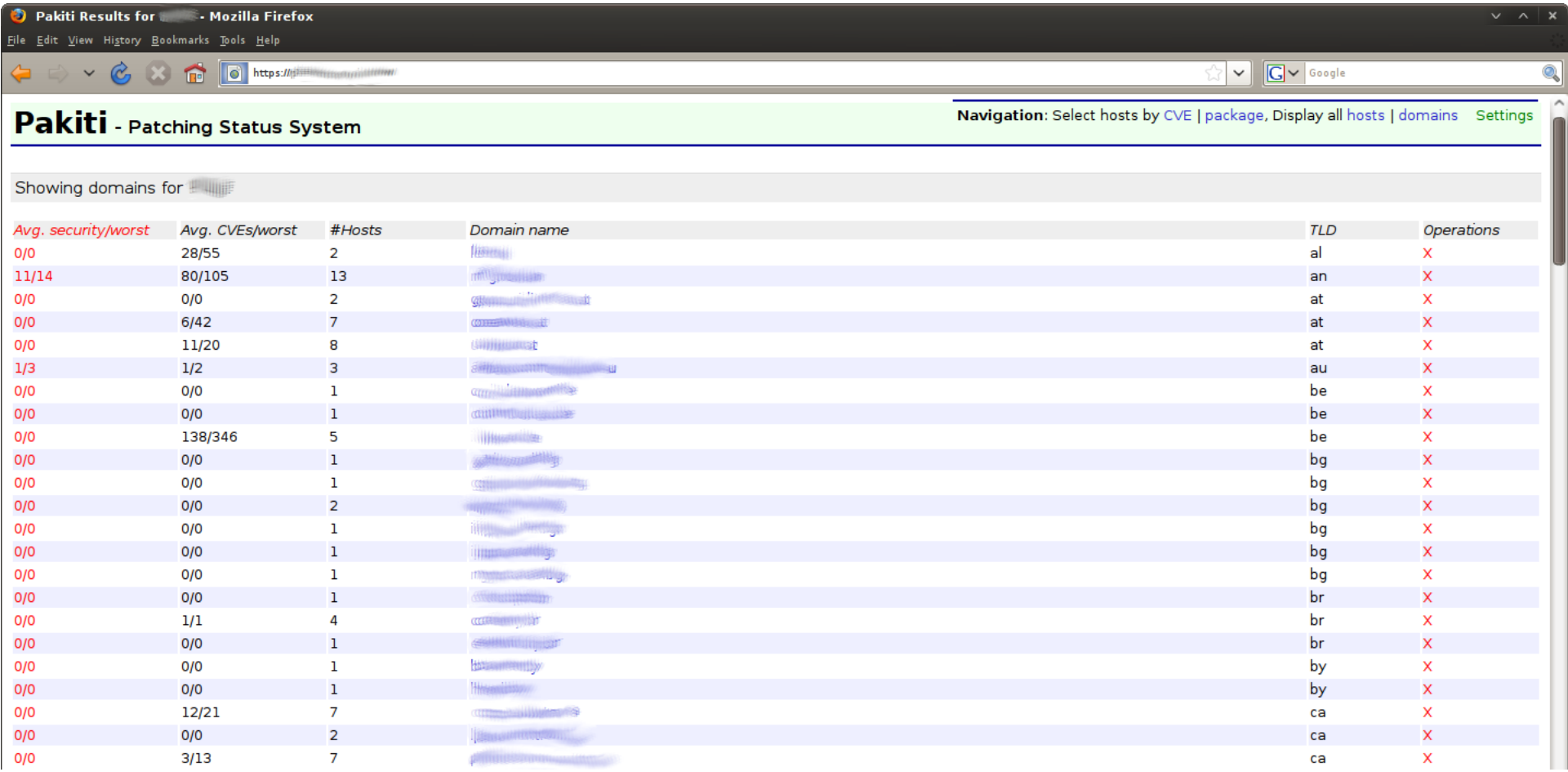
Pakiti v3

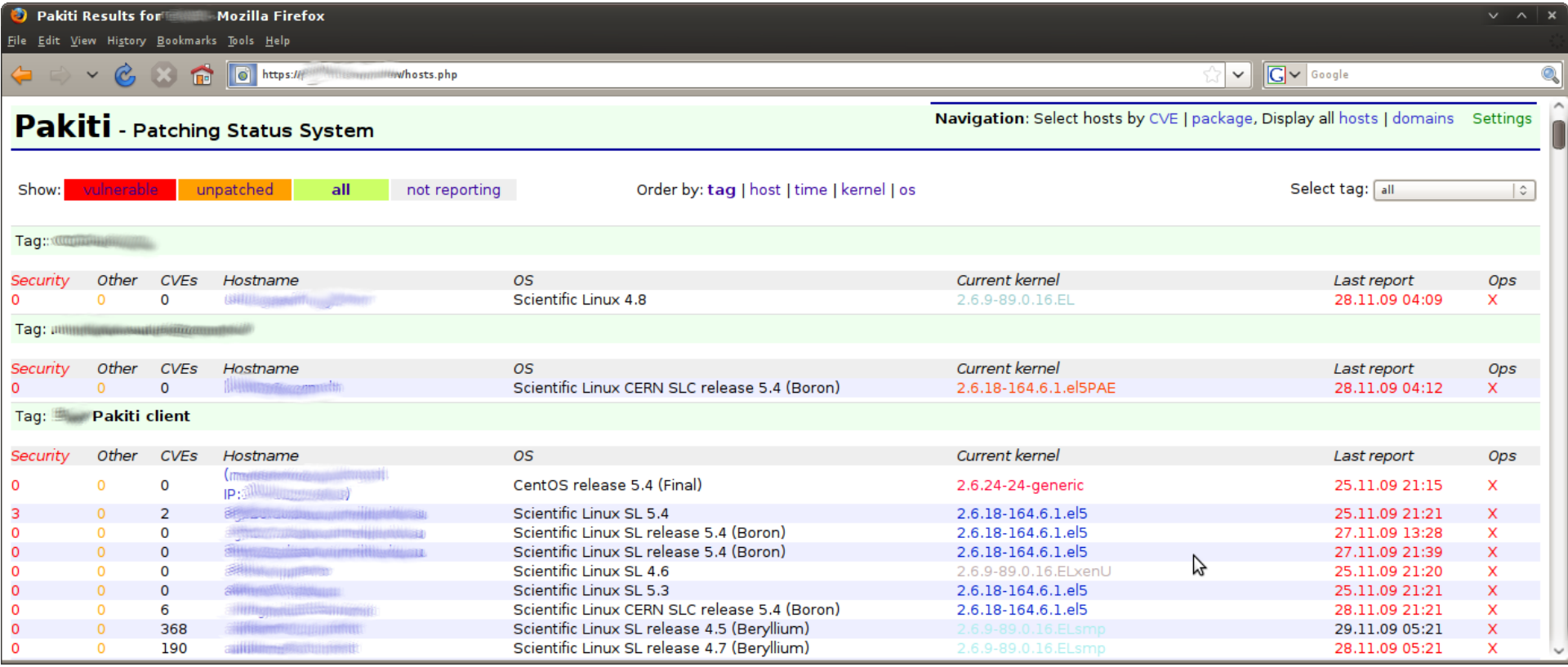
- **Transaction DB**
- **New DB scheme – faster operations**
- **Configurable OVAL parser**
- **ACL**
- **History**
- **More reporting and statistical views**
- **Notifications**
- **We have prototype of the v3**
  - The design and prototype were made by: me:-), Daniel, Christos and Karol Pogonowski

Open Problems

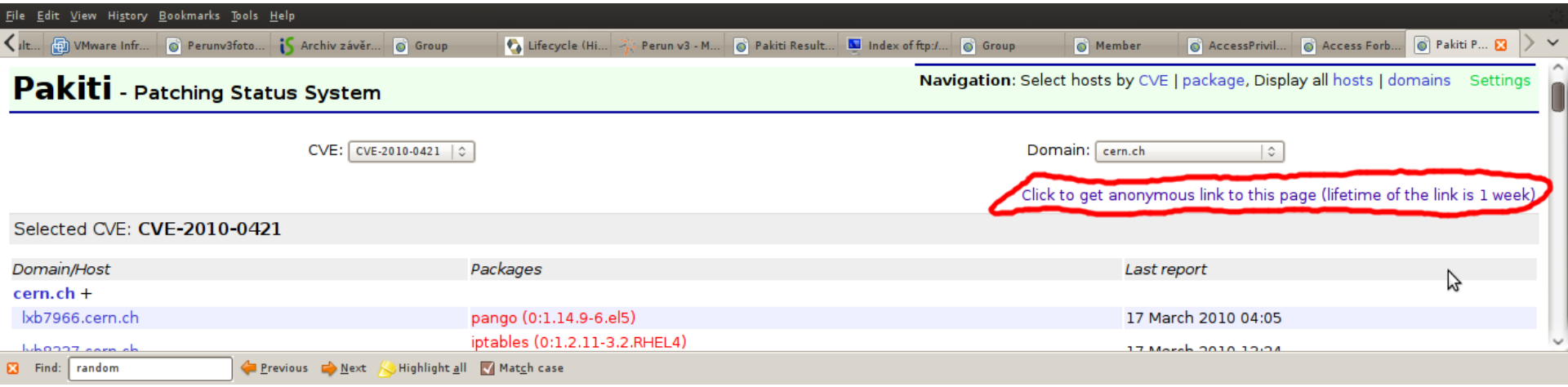
- Client authentication
- Hierarchy of the Pakiti servers

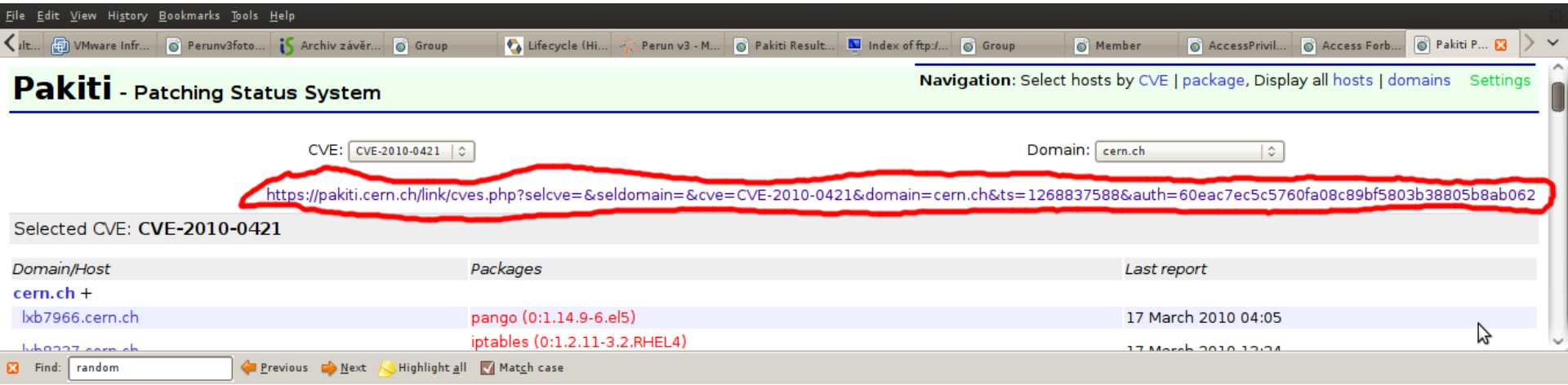
Demo

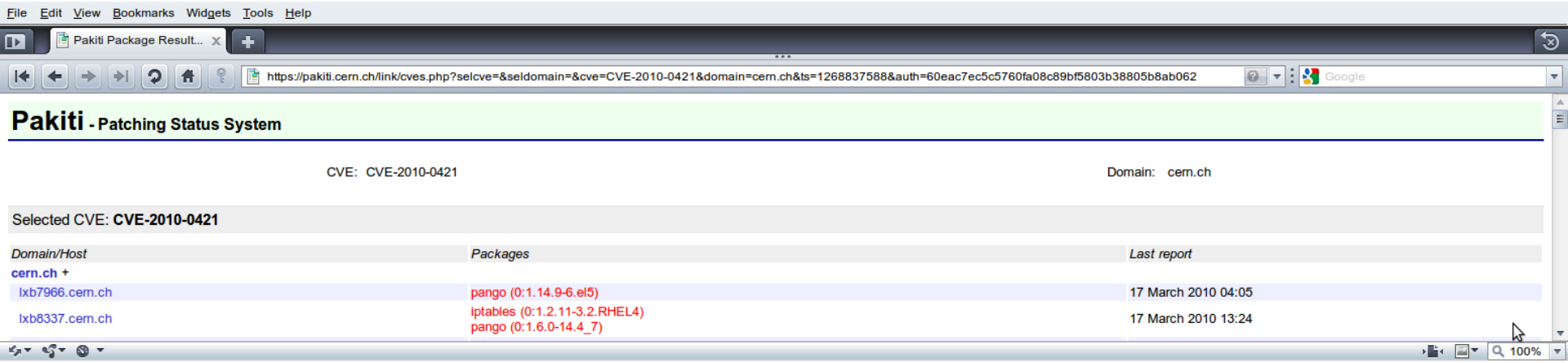

Pakiti Results for - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://
Google
Pakiti - Patching Status System
Navigation: Select hosts by CVE | package, Display all hosts | domains Settings
Showing domains for
Avg. security/worst
Avg. CVEs/worst
#Hosts
Domain name
TLD
Operations
0/0 28/55 2 al X
11/14 80/105 13 an X
0/0 0/0 2 at X
0/0 6/42 7 at X
0/0 11/20 8 at X
1/3 1/2 3 au X
0/0 0/0 1 be X
0/0 0/0 1 be X
0/0 138/346 5 be X
0/0 0/0 1 bg X
0/0 0/0 1 bg X
0/0 0/0 2 bg X
0/0 0/0 1 bg X
0/0 0/0 1 bg X
0/0 0/0 1 bg X
0/0 0/0 1 br X
0/0 1/1 4 br X
0/0 0/0 1 br X
0/0 0/0 1 by X
0/0 0/0 1 by X
0/0 12/21 7 ca X
0/0 0/0 2 ca X
0/0 3/13 7 ca X

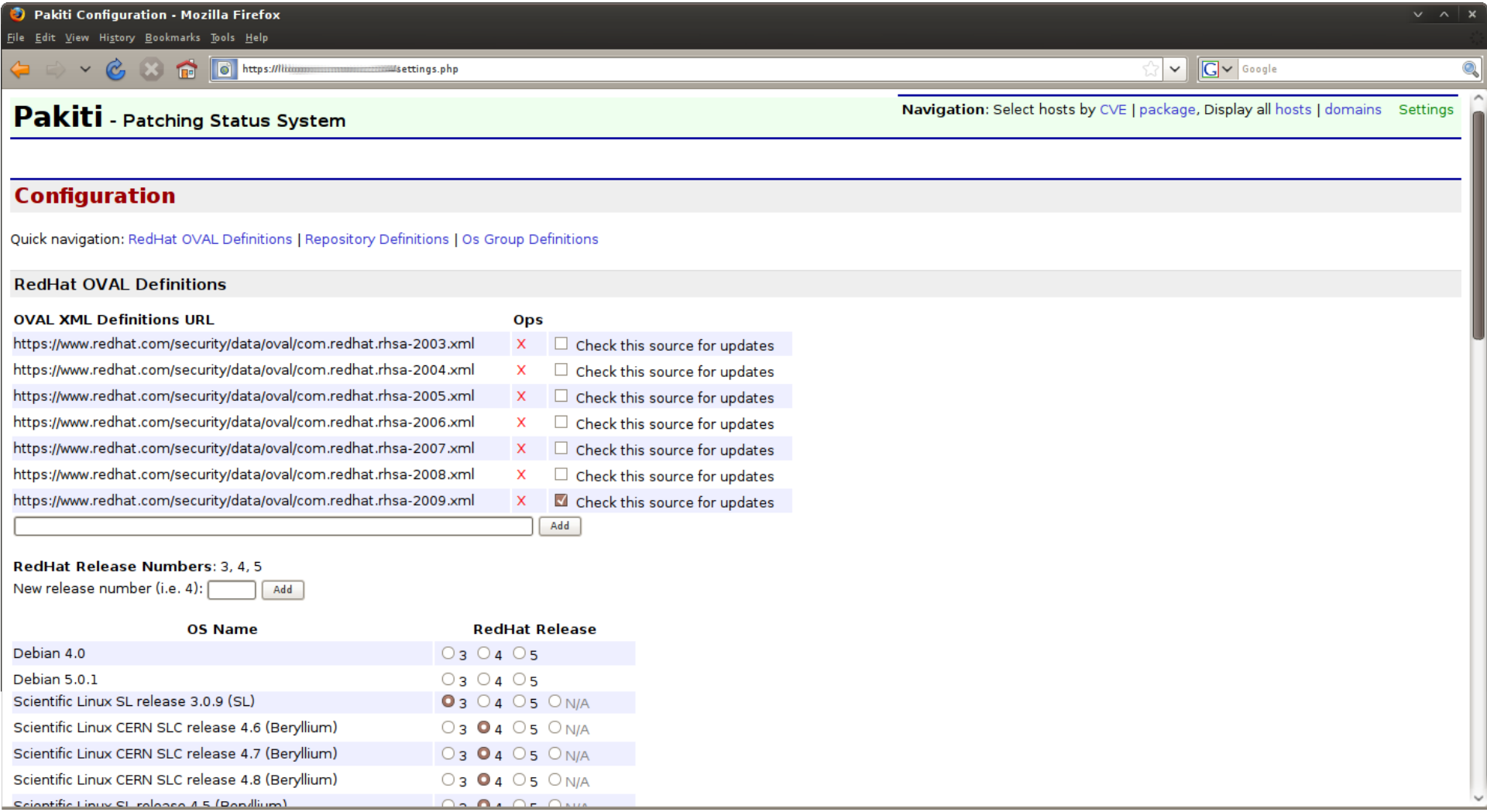

Pakiti Results for [redacted] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]/hosts.php
Google
Pakiti - Patching Status System
Navigation: Select hosts by CVE | package, Display all hosts | domains Settings
Show: vulnerable unpatched all not reporting
Order by: tag | host | time | kernel | os
Select tag: all
Tag:: [redacted]
Security Other CVEs Hostname OS Current kernel Last report Ops
0 0 0 [redacted] Scientific Linux 4.8 2.6.9-89.0.16.EL 28.11.09 04:09 X
Tag: [redacted]
Security Other CVEs Hostname OS Current kernel Last report Ops
0 0 0 [redacted] Scientific Linux CERN SLC release 5.4 (Boron) 2.6.18-164.6.1.el5PAE 28.11.09 04:12 X
Tag: [redacted] Pakiti client
Security Other CVEs Hostname OS Current kernel Last report Ops
0 0 0 ([redacted] IP: [redacted]) CentOS release 5.4 (Final) 2.6.24-24-generic 25.11.09 21:15 X
3 0 2 [redacted] Scientific Linux SL 5.4 2.6.18-164.6.1.el5 25.11.09 21:21 X
0 0 0 [redacted] Scientific Linux SL release 5.4 (Boron) 2.6.18-164.6.1.el5 27.11.09 13:28 X
0 0 0 [redacted] Scientific Linux SL release 5.4 (Boron) 2.6.18-164.6.1.el5 27.11.09 21:39 X
0 0 0 [redacted] Scientific Linux SL 4.6 2.6.9-89.0.16.ELxenU 25.11.09 21:20 X
0 0 0 [redacted] Scientific Linux SL 5.3 2.6.18-164.6.1.el5 25.11.09 21:21 X
0 0 6 [redacted] Scientific Linux CERN SLC release 5.4 (Boron) 2.6.18-164.6.1.el5 28.11.09 21:21 X
0 0 368 [redacted] Scientific Linux SL release 4.5 (Beryllium) 2.6.9-89.0.16.ELsmp 29.11.09 05:21 X
0 0 190 [redacted] Scientific Linux SL release 4.7 (Beryllium) 2.6.9-89.0.16.ELsmp 28.11.09 05:21 X

Anonymous Links






File Edit View Bookmarks Widgets Tools Help
Pakiti Package Result...
https://pakiti.cern.ch/link/cves.php?selcve=&seldomain=&cve=CVE-2010-0421&domain=cern.ch&ts=1268837588&auth=60eac7ec5c5760fa08c89bf5803b38805b8ab062
Pakiti - Patching Status System
CVE: CVE-2010-0421
Domain: cern.ch
Selected CVE: CVE-2010-0421
Domain/Host
Packages
Last report
cern.ch +
lxb7966.cern.ch
pango (0:1.14.9-6.el5)
17 March 2010 04:05
lxb8337.cern.ch
iptables (0:1.2.11-3.2.RHEL4)
pango (0:1.6.0-14.4_7)
17 March 2010 13:24
100%

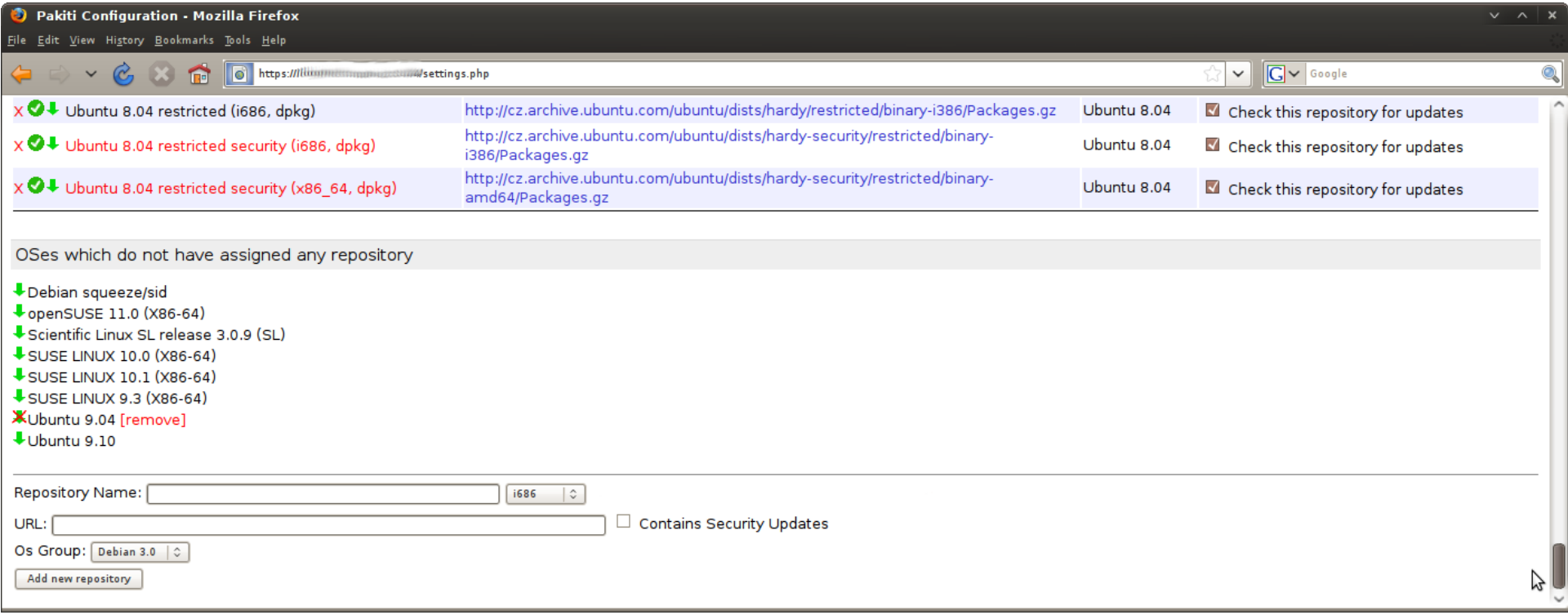

Pakiti Configuration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]settings.php
Google
Pakiti - Patching Status System
Navigation: Select hosts by CVE | package, Display all hosts | domains Settings
Configuration
Quick navigation: RedHat OVAL Definitions | Repository Definitions | Os Group Definitions
RedHat OVAL Definitions
OVAL XML Definitions URL
Ops
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2003.xml X Check this source for updates
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2004.xml X Check this source for updates
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2005.xml X Check this source for updates
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2006.xml X Check this source for updates
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2007.xml X Check this source for updates
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2008.xml X Check this source for updates
https://www.redhat.com/security/data/oval/com.redhat.rhsa-2009.xml X Check this source for updates
Add
RedHat Release Numbers: 3, 4, 5
New release number (i.e. 4): Add
OS Name
RedHat Release
Debian 4.0 3 4 5
Debian 5.0.1 3 4 5
Scientific Linux SL release 3.0.9 (SL) 3 4 5 N/A
Scientific Linux CERN SLC release 4.6 (Beryllium) 3 4 5 N/A
Scientific Linux CERN SLC release 4.7 (Beryllium) 3 4 5 N/A
Scientific Linux CERN SLC release 4.8 (Beryllium) 3 4 5 N/A

Os Group Definitions

OS Group Name	Associated OSes
X Debian 3.0	Add OS
X Debian 4.0	Add OS Debian 4.0 [remove]
X Debian 5.0	Add OS Debian 5.0.1 [remove] Debian 5.0.2 [remove] Debian 5.0.3 [remove]
X SL 4.5	Add OS Scientific Linux SL release 4.5 (Beryllium) [remove]
X SL 4.6	Add OS Scientific Linux SL release 4.6 (Beryllium) [remove]
X SL 4.7	Add OS Scientific Linux SL release 4.7 (Beryllium) [remove]

Repository Definitions

Repository Name	Repository URL	OS Group	
Debian 4.0 i686 contrib (i686, dpkg)	http://ftp.zcu.cz/mirrors/debian/dists/etch/contrib/binary-i386/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 i686 contrib sec (i686, dpkg)	http://security.debian.org/debian-security/dists/etch/updates/contrib/binary-i386/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 i686 main (i686, dpkg)	http://ftp.zcu.cz/mirrors/debian/dists/etch/main/binary-i386/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 i686 main sec (i686, dpkg)	http://security.debian.org/debian-security/dists/etch/updates/main/binary-i386/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 x86_64 contrib (x86_64, dpkg)	http://ftp.zcu.cz/mirrors/debian/dists/etch/contrib/binary-amd64/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 x86_64 contrib sec (x86_64, dpkg)	http://security.debian.org/debian-security/dists/etch/updates/contrib/binary-amd64/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 x86_64 main (x86_64, dpkg)	http://ftp.zcu.cz/mirrors/debian/dists/etch/main/binary-amd64/Packages.gz	Debian 4.0	Check this repository for updates
Debian 4.0 x86_64 main sec (x86_64, dpkg)	http://security.debian.org/debian-security/dists/etch/updates/main/binary-amd64/Packages.gz	Debian 4.0	Check this repository for updates
Debian 5.0 i686 contrib sec (i686, dpkg)	http://security.debian.org/debian-security/dists/lenny/updates/contrib/binary-i386/Packages.gz	Debian 5.0	Check this repository for updates
Debian 5.0 i686 main sec (i686, dpkg)	http://security.debian.org/debian-security/dists/lenny/updates/main/binary-i386/Packages.gz	Debian 5.0	Check this repository for updates
Debian 5.0 i686 non-free sec (i686, dpkg)	http://security.debian.org/debian-security/dists/lenny/updates/non-free/binary-i386/Packages.gz	Debian 5.0	Check this repository for updates
Debian 5.0 x86_64 contrib sec (x86_64, dpkg)	http://security.debian.org/debian-security/dists/lenny/updates/contrib/binary-amd64/Packages.gz	Debian 5.0	Check this repository for updates
Debian 5.0 x86_64 main sec (x86_64, dpkg)	http://security.debian.org/debian-security/dists/lenny/updates/main/binary-amd64/Packages.gz	Debian 5.0	Check this repository for updates
Debian 5.0 x86_64 non-free sec (x86_64, dpkg)	http://security.debian.org/debian-security/dists/lenny/updates/non-free/binary-amd64/Packages.gz	Debian 5.0	Check this repository for updates
OpenSuSE 11.0 (x86_64, rpm)	ftp://ftp5.gwdg.de/pub/linux/suse/opensuse/update/11.0/repodata/primary.xml.gz	SuSE 11.0	Check this repository for updates
SL 4.5 CERN os (i686, rpm)	http://ftp.scientificlinux.org/linux/scientific/45/i386/SL/RPMS/repodata/primary.xml.gz	SL 4.5	Check this repository for updates
SL 4.5 CERN os (x86_64, rpm)	http://ftp.scientificlinux.org/linux/scientific/45/x86_64/SL/RPMS/repodata/primary.xml.gz	SL 4.5	Check this repository for updates
SL 4.5 CERN updates (x86_64, rpm)	http://ftp.scientificlinux.org/linux/scientific/45/x86_64/errata/SL/RPMS/repodata/primary.xml.gz	SL 4.5	Check this repository for updates
SL 4.5 CERN updates (i686, rpm)	http://ftp.scientificlinux.org/linux/scientific/45/i386/errata/SL/RPMS/repodata/primary.xml.gz	SL 4.5	Check this repository for updates
SL 4.6 CERN os (x86_64, rpm)	http://ftp.scientificlinux.org/linux/scientific/46/x86_64/SL/RPMS/repodata/primary.xml.gz	SL 4.6	Check this repository for updates
SL 4.6 CERN os (i686, rpm)	http://ftp.scientificlinux.org/linux/scientific/46/i386/SL/RPMS/repodata/primary.xml.gz	SL 4.6	Check this repository for updates
SL 4.6 CERN updates (x86_64, rpm)	http://ftp.scientificlinux.org/linux/scientific/46/x86_64/errata/SL/RPMS/repodata/primary.xml.gz	SL 4.6	Check this repository for updates
SL 4.6 CERN updates (i686, rpm)	http://ftp.scientificlinux.org/linux/scientific/46/i386/errata/SL/RPMS/repodata/primary.xml.gz	SL 4.6	Check this repository for updates
SL 4.7 CERN updates (x86_64, rpm)	http://ftp.scientificlinux.org/linux/scientific/47/x86_64/errata/SL/RPMS/repodata/primary.xml.gz	SL 4.7	Check this repository for updates
SL 4.8 CERN os (i686, rpm)	http://ftp.scientificlinux.org/linux/scientific/48/i386/SL/RPMS/repodata/primary.xml.gz	SL 4.8	Check this repository for updates
SL 4.8 CERN os (x86_64, rpm)	http://ftp.scientificlinux.org/linux/scientific/48/x86_64/SL/RPMS/repodata/primary.xml.gz	SL 4.8	Check this repository for updates
SL 4.8 CERN updates (i686, rpm)	http://ftp.scientificlinux.org/linux/scientific/48/i386/errata/SL/RPMS/repodata/primary.xml.gz	SL 4.8	Check this repository for updates


Pakiti Configuration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]/settings.php
Google
X Ubuntu 8.04 restricted (i686, dpkg)
http://cz.archive.ubuntu.com/ubuntu/dists/hardy/restricted/binary-i386/Packages.gz
Ubuntu 8.04
Check this repository for updates
X Ubuntu 8.04 restricted security (i686, dpkg)
http://cz.archive.ubuntu.com/ubuntu/dists/hardy-security/restricted/binary-i386/Packages.gz
Ubuntu 8.04
Check this repository for updates
X Ubuntu 8.04 restricted security (x86_64, dpkg)
http://cz.archive.ubuntu.com/ubuntu/dists/hardy-security/restricted/binary-amd64/Packages.gz
Ubuntu 8.04
Check this repository for updates
OSes which do not have assigned any repository
Debian squeeze/sid
openSUSE 11.0 (X86-64)
Scientific Linux SL release 3.0.9 (SL)
SUSE LINUX 10.0 (X86-64)
SUSE LINUX 10.1 (X86-64)
SUSE LINUX 9.3 (X86-64)
Ubuntu 9.04 [remove]
Ubuntu 9.10
Repository Name:
i686
URL:
Contains Security Updates
Os Group:
Debian 3.0
Add new repository