

Pakiti

Ursula Epting



STEINBUCH CENTRE FOR COMPUTING - SCC



Outline

- Pakiti – what is it?
- What is it good for?
- Screenshots
- Conclusion
- Links

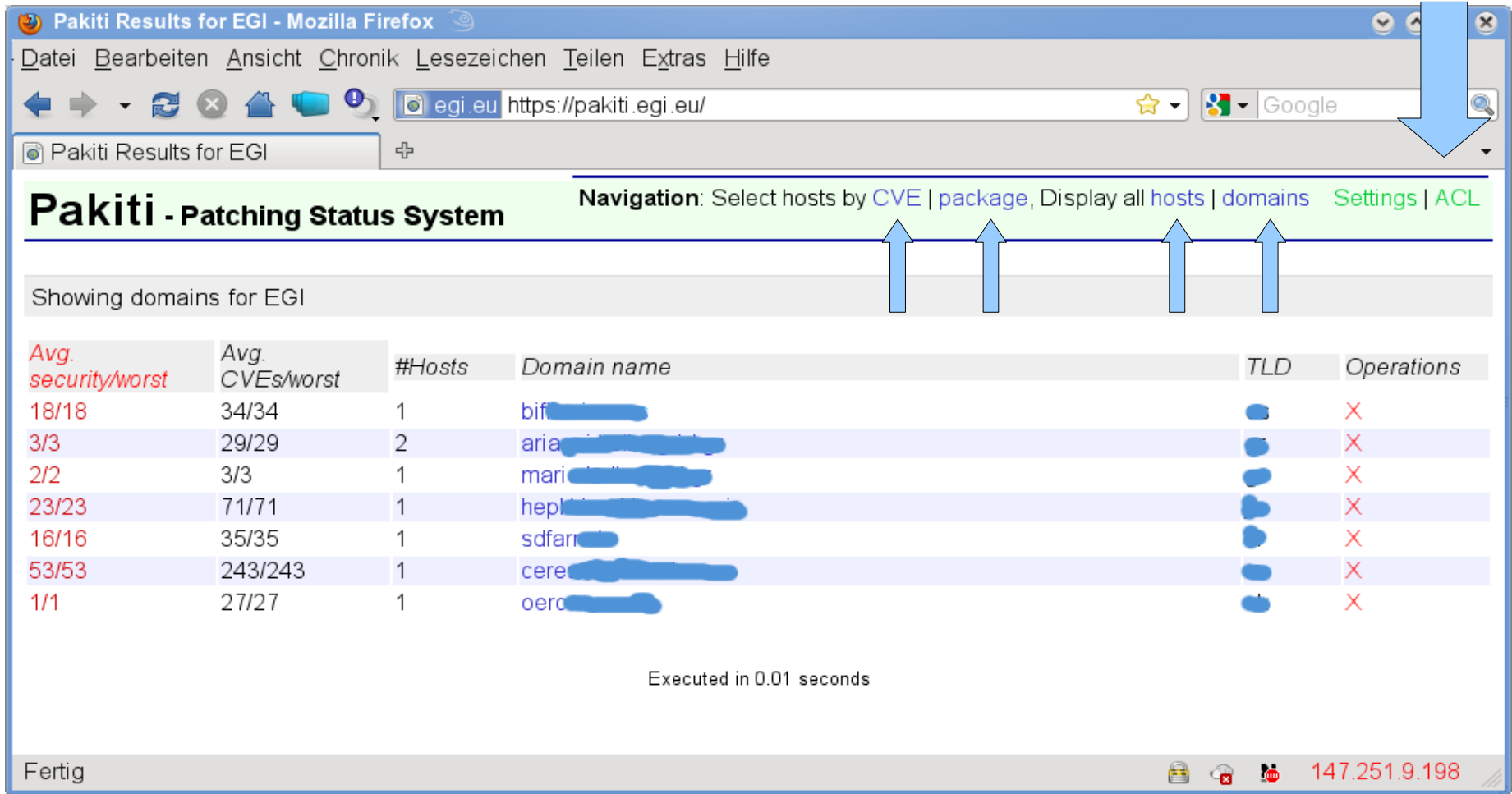
Pakiti – what is it?

- Open source tool to check patching status
 - <https://www.sf.net/projects/pakiti> [1]
 - <http://pakiti.sourceforge.net/> [2]
 - Any site can run its own Pakiti server to monitor internal machines
- Server evaluates packages installed on clients
 - Detects security patches not applied
 - Correlates packet version with vulnerabilities
 - Allows for searching for particular vulnerabilities (CVE - Common Vulnerabilities and Exposures)

Pakiti – What is it good for?

- You can easily have a local installation and check your hosts
 - You can see which hosts have which vulnerabilities
 - You can apply patches where needed
-
- Proved very useful last year in EGEE project, critical kernel vulnerability (CVE-2009-2692, CVE-2009-2698)
→ sites with vulnerable kernels have been identified and were requested to patch their systems
 - Now EGI-CSIRT operates Pakiti server for EGI-inspire [3]
 - Information collected with Nagios probes (WNs)
 - Only EGI-CSIRT members allowed to access

Screenshot Pakiti Start Page



Pakiti Results for EGI - Mozilla Firefox

File Bearbeiten Ansicht Chronik Lesezeichen Teilen Extras Hilfe

egi.eu https://pakiti.egi.eu/

Pakiti Results for EGI

Pakiti - Patching Status System

Navigation: Select hosts by [CVE](#) | [package](#), Display all [hosts](#) | [domains](#) [Settings](#) | [ACL](#)

Showing domains for EGI

Avg. security/worst	Avg. CVEs/worst	#Hosts	Domain name	TLD	Operations
18/18	34/34	1	bif[REDACTED]	[REDACTED]	X
3/3	29/29	2	aria[REDACTED]	[REDACTED]	X
2/2	3/3	1	mari[REDACTED]	[REDACTED]	X
23/23	71/71	1	hepl[REDACTED]	[REDACTED]	X
16/16	35/35	1	sdfar[REDACTED]	[REDACTED]	X
53/53	243/243	1	cere[REDACTED]	[REDACTED]	X
1/1	27/27	1	oerc[REDACTED]	[REDACTED]	X

Executed in 0.01 seconds

Fertig

147.251.9.198

Screenshot Pakiti Hosts

Pakiti Results for EGI - Mozilla Firefox

eg_i.eu https://pakiti.egi.eu/hosts.php

Pakiti - Patching Status System

Navigation: Select hosts by [CVE](#) | [package](#), Display all [hosts](#) | [domains](#) [Settings](#) | [ACL](#)

Show: **vulnerable** | unpatched | **all** | not reporting

Order by: **tag** | hostname | kernel | os

Select tag: all

Expand all +
Tag: Nagios +

Security	Other	CVEs	Hostname	OS	Current kernel	Last report	Ops
53	151	243	glite-1 (IP:)	CentOS Linux 5	2.6.18-128.1.14.el5xen	8.9.10 07:16	X
1	0	27	qua (IP:)	Scientific Linux 4.8	2.6.9-89.0.16.ELsmp	8.9.10 02:00	X
23	8	71	qx1 (IP:)	Scientific Linux 5.5	2.6.18-194.3.1.el5	8.9.10 01:31	X
3	0	29	wn001	Scientific Linux 5.4	2.6.18-164.15.1.el5	8.9.10 01:23	X
3	0	29	wn003	Scientific Linux 5.4	2.6.18-164.15.1.el5	8.9.10 01:23	X
16	0	35	wn003	Scientific Linux 5.2	2.6.18-194.8.1.el5	8.9.10 18:47	X
2	0	3	wn024	Scientific Linux 5.4	2.6.18-194.11.1.el5	8.9.10 01:42	X
18	6	34	wn32- (server2 IP:)	Scientific Linux 5.5	2.6.18-194.8.1.el5	8.9.10 08:09	X

Statistics

Tag	Hosts	Clean nodes	Unpatched hosts	Vulnerable hosts	Average # security fixes	# security fixes (worse host)	Dead hosts	Last report
Nagios8	8	0	3	8	15	53	0	9 September 2010 13:15

Executed in 0.01 seconds

Fertig

147.251.9.198

Screenshot Pakiti Host Details

Pakiti Results for glite-1.local - Mozilla Firefox <2>

File Edit View Chronik Lesezeichen Teilen Extras Hilfe

egi.eu https://pakiti.egi.eu/host.php?h=glite-1.local&d=2480&tag=Nagios

Pakiti Results for glite-1.local

Pakiti - Patching Status System

Navigation: Select hosts by CVE | package, Display all hosts | domains Settings | ACL

Click to select host Click to select package Click to select CVE Tag: Nagios View: All needed Updates

Selected host: **glite-1** package: all CVE: all

Host/Package name	Installed version	Required version (Security repository, Main repository)	CVEs (Critical, Important, Moderate, Low) Show/Hide CVEs
glite-1 (Domain: Os: CentOS Linux 5 (x86_64) Kernel: 2.6.18-128.1.14.el5xen)			
autofs	1:5.0.1/0.rc2.102	1:5.0.1/0.rc2.143.el5_5.4	
avahi	0:0.6.16/1.el5_2.1	0:0.6.16/9.el5_5	CVE-2009-0758 CVE-2010-2244
avahi-compat-libdns_sd	0:0.6.16/1.el5_2.1	0:0.6.16/9.el5_5	CVE-2009-0758 CVE-2010-2244
crash	4:0.7.2.3.el5.centos.1	0:4.1.2/4.el5.centos.1	
cups	1:1.3.7/18.el5_5.7	1:1.3.7/18.el5_5.7	CVE-2010-0540 CVE-2010-0542 CVE-2010-1748 CVE-2010-0302 CVE-2009-2820 CVE-2009-3553 CVE-2009-3608 CVE-2009-3609
cups-libs	1:1.3.7/8.el5_3.6	1:1.3.7/18.el5_5.7	CVE-2010-0540 CVE-2010-0542 CVE-2010-1748 CVE-2010-0302 CVE-2009-2820 CVE-2009-3553 CVE-2009-3608 CVE-2009-3609
db4	0:4.3.29/9.fc6	0:4.3.29/10.el5_5.2	
dbus-glib	0:0.73/8.el5	0:0.73/10.el5_5	CVE-2010-1172
device-mapper-multipath	0:0.4.7/23.el5_3.4	0:0.4.7/34.el5_5.4	
dhclient	12:3.0.5/18.el5	12:3.0.5/23.el5_5.1	
dhcp	12:3.0.5/18.el5	12:3.0.5/23.el5_5.1	
freetype	0:2.2.1/21.el5_3	0:2.2.1/26.el5_5	CVE-2010-2498 CVE-2010-2499 CVE-2010-2500 CVE-2010-2519 CVE-2010-2527 CVE-2010-2541 CVE-2010-1797
gnupg	0:1.4.5/14	0:1.4.5/14.el5_5.1	
gnutls	0:1.4.1/3.el5_2.1	0:1.4.1/3.el5_4.8	CVE-2009-2409 CVE-2009-3555 CVE-2009-2730 CVE-2009-1890 CVE-2009-1891 CVE-2008-1678 CVE-2009-1195 CVE-2009-3094 CVE-2009-3095 CVE-2009-3555 CVE-2010-0408 CVE-2010-0434 CVE-2010-1452 CVE-2010-2791
insec-tools	0:0.6.5/13.el5_3.1	0:0.6.5/14.el5_5.5	
Fertig			147.251.9.198

Note that all unpatched hosts are
vulnerable!

Which tools are used at your site
for patch management?

Links

[1] <https://www.sf.net/projects/pakiti>

[2] <http://pakiti.sourceforge.net/>
(with installation instructions)

[3] <https://pakiti.egi.eu/>
(restricted access NGI security officers only!)