



MTA SZTAKI

COMPUTER AND AUTOMATION RESEARCH INSTITUTE
HUNGARIAN ACADEMY OF SCIENCES

MAGYAR TUDOMÁNYOS AKADÉMIA
SZÁMÍTÁSTECHNIKAI ÉS
AUTOMATIZÁLÁSI KUTATÓINTÉZET

User Manual

GSSVA

(Grid Site Software
Vulnerability Analyzer)

S. Acs, M. Kozlovsky, Z.
Balaton



MTA SZTAKI
MTA SZTAKI - Laboratory of Parallel and Distributed Systems
H-1111 Budapest, Kende u. 13-17, Hungary
H-1518 Budapest, P.O.B. 63, Hungary
Phone/fax: (+36 1) 329 7864

Table of contents

Table of contents.....	2
1 About the software.....	3
1.1 The goal of the software.....	3
1.2 Contacts.....	3
2 How can I use?.....	4
2.1 Prerequisites.....	4
2.2 Registration.....	4
2.3 The web address of the service	4
3 Examples.....	5
4 Acknowledgement.....	7
5 References.....	8

1 About the software

1.1 The goal of the software

In order to increase the security level of the grid infrastructure a security assessment tool: Grid Site Software Vulnerability Analyzer (GSSVA) has been designed and implemented by the Laboratory of Parallel and Distributed Systems (LPDS) at MTA SZTAKI. This developed monitoring tool overcomes the issues with communication through firewalls and client side installation without root privileges. GSSVA is using basic grid services and modified PAKITI status monitoring system. It can automatically explore the installed Linux packages locating on the grid machines.

1.2 Contacts

The contact email address is: "gssva_service@lpds.sztaki.hu".

2 How can I use?

2.1 Prerequisites

a, You must have valid certificate (imported to your web browser).

b, You should be registered at HGSM (<https://hgsm.grid.org.tr/>).

2.2 Registration

Send an email to the contact address (gssva_service@lpds.sztaki.hu) and the administrators at SZTAKI will register you into the system and they will send you feedback.

2.3 The web address of the service

After the feedback you can use the service via "<http://www.lpds.sztaki.hu/gssva>".

3 Examples

Pakiti: "security" view - hosts for TESZT (31 October 2008 22:20)

Order by: tag Choose view: deployment security

Tag: test vers

Scientific Linux 4

Vulnerable RPMs	CVEs	hostname	current kernel	last report	version
12	15	g-ena_1	2.6.18.8-xen-3.2.1-2	7 September 2008 19:44	g-ena_vers
4	4	g-ena_2	2.6.18.8-xen-3.2.1-2	30 September 2008 17:22	g-ena_vers
7	11	G-E_1	2.6.18.8-xen-3.2.1-2	24 October 2008 22:51	G.-E.vers

Executed in 0.01 seconds

Figure 1: Security view

The tool provides a graphical user interface to visualize security assessment results for grid administrators. It can present a short summary of the vulnerabilities of the selected computer (See at Figure 1) or give a hyper-link to a security web page where administrator can learn more about the problem.

Pakiti Package Results for TESZT: 31 October 2008 22:21 "security" view

Host: [g-ena_1](#)

deployment security Hostname: Package: CVE: All Tag: Domain: All

Show RPMs Show text

Scientific Linux 4

(7 September 2008), [g-ena_1](#)

[CVE-2008-1447](#) [CVE-2008-1946](#) [CVE-2008-3651](#) [CVE-2008-3652](#) [CVE-2008-2136](#) [CVE-2006-4145](#) [CVE-2008-2812](#) [CVE-2008-2327](#) [CVE-2006-2193](#)
[CVE-2008-3281](#) [CVE-2008-2935](#) [CVE-2007-5794](#)

Display all hosts

Figure 2: Security references

We can choose a node from the list and we can see the security problems references.

Pakiti Package Results for TESZT: 31 October 2008 22:22 "security" view

deployment	security	Hostname: All	Package: All	CVE: All Show RPMs Hide text	Tag: All	Domain: All
------------	----------	---------------	--------------	------------------------------------	----------	-------------

Scientific Linux 4

(7 September 2008), [CVE-2008-1447](#) [CVE-2008-1946](#) [CVE-2008-3651](#) [CVE-2008-3652](#) [CVE-2008-2136](#) [CVE-2006-4145](#) [CVE-2008-2812](#) [CVE-2008-2327](#) [CVE-2006-2193](#) [CVE-2008-3281](#)

The libxml2 packages provide a library that allows you to manipulate XML files. It includes support to read, modify, and write XML and HTML files.

A denial of service flaw was found in the way libxml2 processes certain content. If an application linked against libxml2 processes malformed XML content, it could cause the application to stop responding. (CVE-2008-3281)

Red Hat would like to thank Andreas Solberg for responsibly disclosing this issue.

All users of libxml2 are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue.

(30 September 2008), [CVE-2008-1372](#) [CVE-2008-3529](#)

Figure 3: Text mode

We can switch to text mode which generate a short description about the security problem.

4 Acknowledgement

This work is supported by the European Commission under the FP7 Research Infrastructure, SEE-GRID-SCI project, contract No. 211338.

5 References

- [1] S. Acs, M. Kozlovzsky, Z. Balaton: PARENG conference: "The First International Conference on Parallel, Distributed and Grid Computing for Engineering", paper: "Automation of Security Analysis for Service Grid Systems", doi:10.4203/ccp.90.25, <http://dx.doi.org/10.4203/ccp.90.25> - 2009
- [2] XXIX. Országos Tudományos Diákköri Konferencia, (Nationwide Scientific Conference for Undergraduate Students) - 2009
- [3] Thesis of bachelor's degree, S. Acs: Vulnerability Monitoring in Grid Systems - 2009
- [4] SEE-GRID-SCI WIKI, http://wiki.egee-see.org/index.php/JRA1_Commonalities