

# Keeping Gentoo Secure

Open Source Security and how Gentoo does it

Alex Legler <a3li@gentoo.org>

Gentoo Linux Security Team

Gentoo Miniconf Prague  
October 2012



## 1 Introduction

## 2 Open Source Security

## 3 ...in Gentoo

- Processes
- Tools

## 4 Keeping your system safe

## 5 Thanks



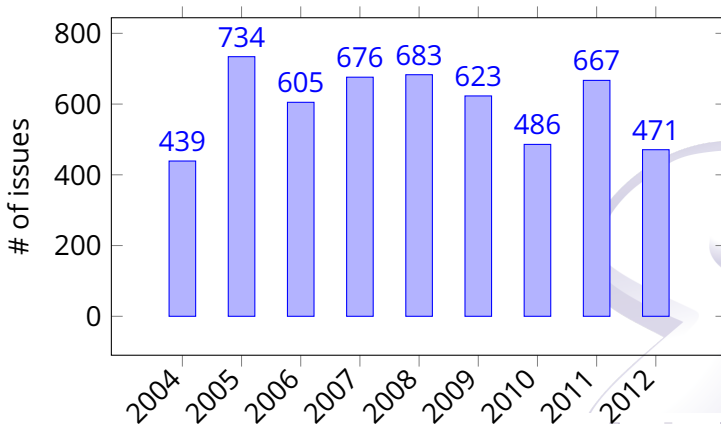
# Hi!

- **I'm Alex '*a3li*' Legler**
- Living and studying in Würzburg, Germany
- Gentoo developer since 2009
  - Involved in Ruby packaging, Security, Infra and PR
  - Board member of the Gentoo e.V. association in Germany
  - [wiki.gentoo.org](http://wiki.gentoo.org) is mostly my fault
  - Currently leading the Security team



# Why is this important?

Handled security issues on bugs.gentoo.org per year



# Vulnerability Disclosure Methods

## Responsible disclosure

- Authors get private notification
- Fix expected in  $\leq$  4-6 weeks
- Leads to a coordinated release or full disclosure

## Full disclosure

- (Immediate) public release of vulnerability details
- Controversial method

# Vulnerability Disclosure Methods

## Responsible disclosure

- Authors get private notification
- Fix expected in  $\leq$  4-6 weeks
- Leads to a coordinated release or full disclosure

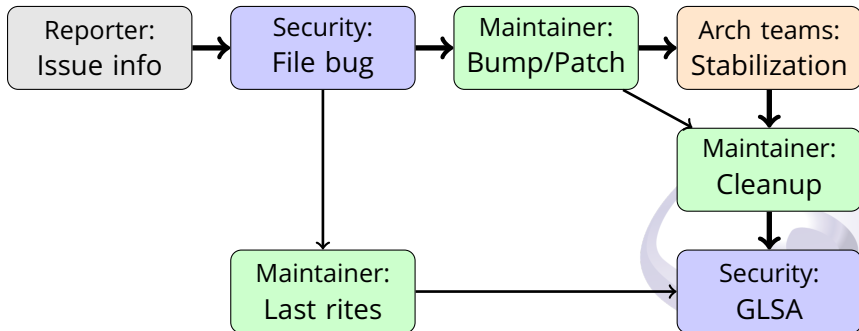
## Full disclosure

- (Immediate) public release of vulnerability details
- Controversial method

# Vulnerability Information Sources

- *Common Vulnerabilities and Exposures* list (CVE)
- Aggregation services (*Secunia*, *packetstorm*)
- Computer Emergency Response Teams (*CERT/CC*, *oCERT*)
- Upstream notification (Release Notes, email)
- Public mailing lists (*oss-sec*, *full-disclosure*, *bugtraq*)
- Coordinated release (via *linux-distros* or upstream directly)
- Peer security teams (especially *RedHat*)
- Bug tracker reports (by users or developers)

# Workflow: From Issue to Advisory





# Workflow: Bug dispatch: Rating issues

## How widespread is the package?

System package	any configuration <b>A</b>	
Common package (>5%)	default config <b>A</b>	specific <b>B</b>
Marginal package (<5%)	default config <b>B</b>	specific <b>C</b>
Package not stable	any configuration ~	

# Workflow: Bug dispatch: Rating issues (2)

## How severe is the issue?

Remote root compromise	<b>0</b>
Active remote user or local root compromise	<b>1</b>
User-assisted remote user compromise	<b>2</b>
Denial of Service, data loss or full information leak	<b>3</b>
XSS, SQLi, partial database leak, others	<b>4</b>

# Workflow: Bug handling: Tracking status

## Example status

Marginal package, remote code execution, being stabled:

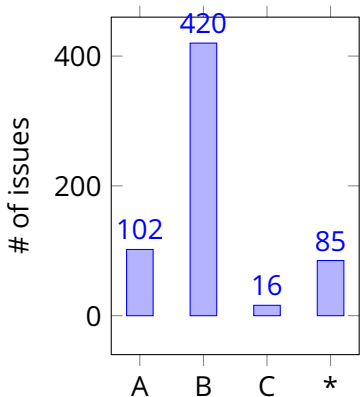
→ B2 [stable]

- [upstream]: Waiting for an upstream fix
- [upstream/ebuild]: Waiting or patching?
- [ebuild]: Updated ebuild pending
- [stable]: Stabilization is performed
- [glsa?]: Deciding whether to release a GLSA
- [(no)glsa]: (no) GLSA released

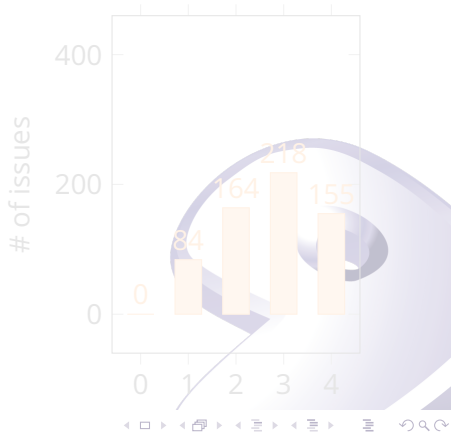


# 2011 issue statistics

## Package importance

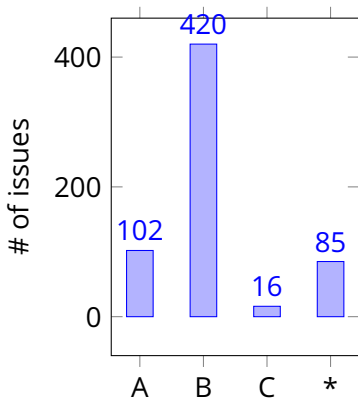


## Issue severity

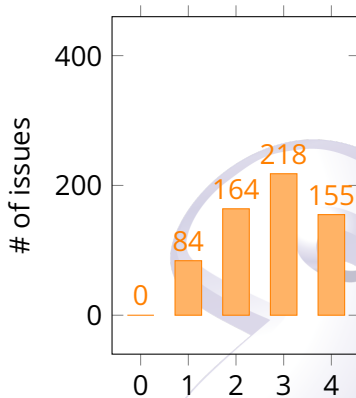


# 2011 issue statistics

## Package importance



## Issue severity



# Tools: CVETool

**CVE-TOOL**

View settings

NEW ASS LAT NFU INV

quicksearch  Filter...

Assign selected CVEs to bug

bug  Assign

New bug from selected CVEs

File a new bug

Mark selected CVEs as...

NFU LATER INVALID

Add a note to selected CVEs

Note

Add note

Info about selected CVEs

Reload table

Back to GLSAMaker

ID	CVE ID	Summary
45200	<b>CVE-2012-5376</b>	The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended
45193	<b>CVE-2012-5354</b>	Mozilla Firefox before 16.0, Thunderbird before 16.0, and SeaMonkey before 2.13 do not properly handle navigation away from a web page th
45019	<b>CVE-2012-5303</b>	Monkey HTTP Daemon 0.9.3 might allow local users to overwrite arbitrary files via a symlink attack on a PID file, as demonstrated by a path
45125	<b>CVE-2012-5272</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45124	<b>CVE-2012-5271</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45123	<b>CVE-2012-5270</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45122	<b>CVE-2012-5269</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45121	<b>CVE-2012-5268</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45120	<b>CVE-2012-5267</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45119	<b>CVE-2012-5266</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45118	<b>CVE-2012-5265</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45117	<b>CVE-2012-5264</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45116	<b>CVE-2012-5263</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45115	<b>CVE-2012-5262</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45114	<b>CVE-2012-5261</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45113	<b>CVE-2012-5260</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45112	<b>CVE-2012-5259</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45111	<b>CVE-2012-5258</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45110	<b>CVE-2012-5257</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45109	<b>CVE-2012-5256</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45108	<b>CVE-2012-5255</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45107	<b>CVE-2012-5254</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45106	<b>CVE-2012-5253</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45105	<b>CVE-2012-5252</b>	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45104	<b>CVE-2012-5251</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45103	<b>CVE-2012-5250</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45102	<b>CVE-2012-5249</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
45101	<b>CVE-2012-5248</b>	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.2
44993	<b>CVE-2012-5240</b>	Buffer overflow in the dissect_tlv function in epan/dissectors/packet-ldp.c in the LDP dissector in Wireshark 1.8.x before 1.8.3 allows remote
44992	<b>CVE-2012-5238</b>	epan/dissectors/packet-ppp.c in the PPP dissector in Wireshark 1.8.x before 1.8.3 uses incorrect OUI data structures during the decoding of

# Tools: GLSAMaker

The screenshot shows the GLSAMaker web interface in a browser. The URL is <https://glsamaker2.gentoo.org/glsas/1949>. The user is logged in as **a3li (Alex Legler)**. The interface has tabs for **New...**, **Requests**, **Drafts**, **Archive**, and **CVETool**. The **Drafts** tab is active, showing a draft titled **Chromium: Multiple vulnerabilities**. The draft is in the **GLSA** state with ID **d00b5322c:r6**. The draft is not ready for sending. The requester is **Pawel Hajdan, Jr. (phajdan.jr)**, the submitter is **Pawel Hajdan, Jr. (phajdan.jr)**, and the editor is **Pawel Hajdan, Jr. (phajdan.jr)**. The draft was created on **Thu, 06 Sep 12 13:01**, submitted on **Sat, 13 Oct 12 21:15**, and edited on **Sat, 13 Oct 12 21:15**. The draft has 4 bugs listed: **433551**, **436234**, **437664**, and **437984**. The comments section shows two comments: one from **Sean Amoss** on **Thu, 06 Sep 12 21:56** asking if it resolves CVE-2012-5376, and another from **Pawel Hajdan, Jr.** on **Sat, 13 Oct 12 21:17** confirming that CVE-2012-5376 is addressed in the release notes. The draft also has a description and an impact section. The interface includes a search bar, a 'Show revision' dropdown, and a 'GLSAMaker VERSION 2' logo.

Field	Content
<b>Access</b>	remote
<b>Severity</b>	normal
<b>Synopsis</b>	Multiple vulnerabilities have been reported in Chromium, some of which may allow execution of arbitrary code.
<b>Unaffected packages</b>	• <code>&gt;=www-client/chromium-22.0.1229.94</code> on * (auto: true)
<b>Vulnerable packages</b>	• <code>&lt;www-client/chromium-22.0.1229.94</code> on * (auto: true)
<b>Background</b>	Chromium is an open source web browser project.
<b>Description</b>	Multiple vulnerabilities have been discovered in Chromium. Please review the CVE identifiers and release notes referenced below for details.
<b>Impact</b>	A remote attacker could entice a user to open a specially crafted web site using Chromium, possibly resulting in the execution of arbitrary code with the privileges of the process, arbitrary file write, a Denial of Service condition, Cross-Site Scripting in SSL interstitial and various Universal Cross-Site Scripting attacks.
	There is no known workaround at this time.

GLSAMaker 2.0 About...

# glsa-check

## Checking a system's overall GLSA status

```
$ glsa-check -l affected
```

[A] means this GLSA was marked as applied (injected),

[U] means the system is not affected and

[N] indicates that the system might be affected.

```
201209-03 [N] PHP: Multiple vulnerabilities ↔  
( dev-lang/php )
```

```
201209-13 [N] libjpeg-turbo: Code execution ↔  
( media-libs/libjpeg-turbo )
```

```
201209-14 [N] file: Denial of Service ↔  
( sys-apps/file )
```



# glsa-check (2)

## Finding an upgrade path

```
$ glsa-check -p affected
Checking GLSA 201209-13
>>> Updates that will be performed:
    media-libs/libjpeg-turbo-1.2.1 (vulnerable: ~-1.2.0)
Checking GLSA 201209-14
>>> Updates that will be performed:
    sys-apps/file-5.11 (vulnerable: sys-apps/file-5.09)
Checking GLSA 201209-03
>>> No upgrade path exists for these packages:
    dev-lang/php-5.3.15
```

# glsa-check (3)

## Advisory details

```
$ glsa-check -d 201206-27
```

```
mini_httpd: Arbitrary code execution
```

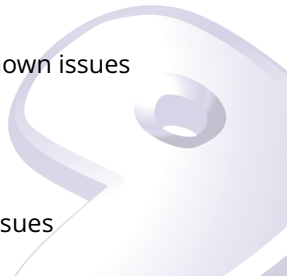
```
=====
Synopsis:  A vulnerability in mini_httpd could allow
           remote attackers to execute arbitrary code.
```

```
...
```

```
Resolution: Gentoo discontinued support for mini_httpd.
            We recommend that users unmerge mini_httpd:
            # emerge --unmerge "www-servers/mini_httpd"
```

# Further efforts

- Gentoo Hardened
  - Gentoo project offering various enhancements to the Kernel and Toolchain
  - <http://hardened.gentoo.org/>
- kernel-check
  - Compares running kernel with a list of known issues
  - Development stalled, volunteers wanted!
- Security Auditing subproject
  - Recent staff addition
  - Gentoo will resume actively looking for issues



# Future plans

- Getting Gentoo certified as *CVE compatible*
- Updating GLSA format
  - Less redundant information
  - Slotting support
- New <http://security.gentoo.org/>
  - Searchable GLSA archive
  - CVE–Package–GLSA mapping
  - Notification service for medium/low severity issues without an advisory



# Thanks!

- **Questions?**
- Want to see the tools live? Ask me!
- The team can be reached via <security@gentoo.org>

Shameless plug: **We need your help!**

- File bugs you find or discover on [bugs.gentoo.org](https://bugs.gentoo.org)
- Help wrangle bugs
- Help draft, review and release advisories
- **Interested?** Contact us (now, not *maybe later!*)

# Thanks!

## ■ Questions?

- Want to see the tools live? Ask me!
- The team can be reached via <security@gentoo.org>

Shameless plug: **We need your help!**

- File bugs you find or discover on [bugs.gentoo.org](https://bugs.gentoo.org)
- Help wrangle bugs
- Help draft, review and release advisories
- **Interested?** Contact us (now, not *maybe later!*)

# Advertisement: Get Merchandise!



- Larry the cow mugs
- Available at the Gentoo booth