

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



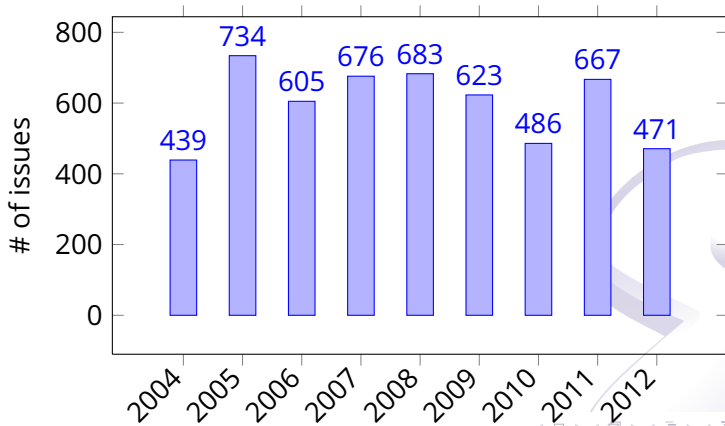
Hi!

- **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 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

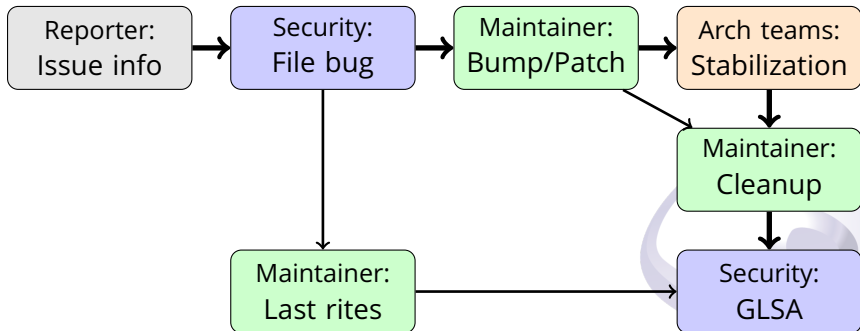
Full disclosure

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

Workflow: Bug dispatch: Rating issues (2)

How severe is the issue?

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

Workflow: Bug handling: Tracking status

Example status

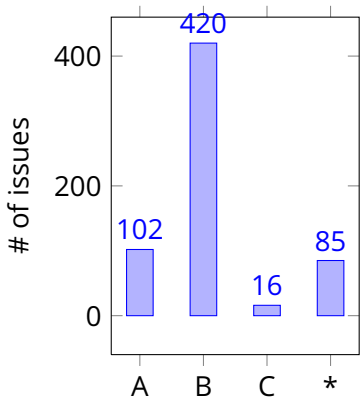
Marginal package, remote code execution, being stabled:
→ B2 [stable]

- [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

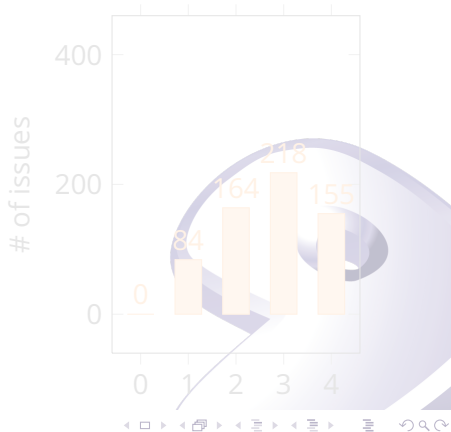


2011 issue statistics

Package importance

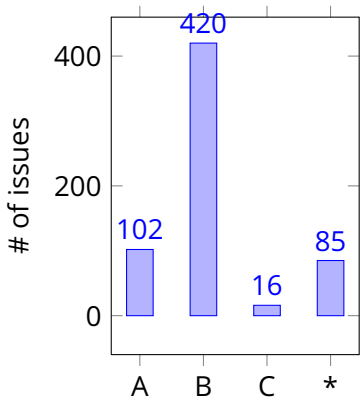


Issue severity

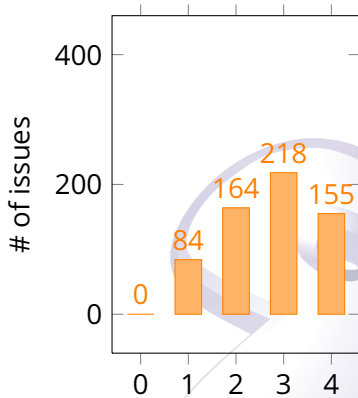


2011 issue statistics

Package importance



Issue severity



Tools: CVETool

CVETool

ID	CVE ID	Summary
45200	CVE-2012-5376	The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended...
45193	CVE-2012-5354	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	CVE-2012-5303	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	CVE-2012-5272	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...
45124	CVE-2012-5271	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...
45123	CVE-2012-5270	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...
45122	CVE-2012-5269	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...
45121	CVE-2012-5268	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...
45120	CVE-2012-5267	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...
45119	CVE-2012-5266	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...
45118	CVE-2012-5265	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...
45117	CVE-2012-5264	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...
45116	CVE-2012-5263	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...
45115	CVE-2012-5262	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...
45114	CVE-2012-5261	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...
45113	CVE-2012-5260	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...
45112	CVE-2012-5259	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...
45111	CVE-2012-5258	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...
45110	CVE-2012-5257	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...
45109	CVE-2012-5256	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...
45108	CVE-2012-5255	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...
45107	CVE-2012-5254	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...
45106	CVE-2012-5253	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...
45105	CVE-2012-5252	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...
45104	CVE-2012-5251	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...
45103	CVE-2012-5250	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...
45102	CVE-2012-5249	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...
45101	CVE-2012-5248	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...
44993	CVE-2012-5240	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	CVE-2012-5238	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 page title is "Chromium: Multiple vulnerabilities". The interface includes a navigation bar with tabs for "New...", "Requests", "Drafts", "Archive", and "CVETool". A search bar is present with the text "Everywhere". The user is logged in as "a3li (Alex Legler)".

The main content area is divided into two columns. The left column contains a table with the following fields:

Field	Content
Access	remote
Severity	normal
Synopsis	Multiple vulnerabilities have been reported in Chromium, some of which may allow execution of arbitrary code.
Unaffected packages	• <code>>=www-client/chromium-22.0.1229.94</code> on * (auto: true)
Vulnerable packages	• <code><www-client/chromium-22.0.1229.94</code> on * (auto: true)
Background	Chromium is an open source web browser project.
Description	Multiple vulnerabilities have been discovered in Chromium. Please review the CVE identifiers and release notes referenced below for details.
Impact	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.

The right column contains the draft details and a list of bugs. The draft title is "GLSA d00b5322c:r6". A status message says "This draft is not ready for sending." The requester is Pawel Hajdan, Jr. (phajdan.jr) on Thu, 06 Sep 12 13:01. The submitter is Pawel Hajdan, Jr. (phajdan.jr) on Sat, 13 Oct 12 21:15. The editor is Pawel Hajdan, Jr. (phajdan.jr) on Sat, 13 Oct 12 21:15.

There are 4 bugs listed:

- 433551** [RFC] <www-client/chromium-21.0.1180.89 multiple vulnerabilit...
- 436234** [RFC] <www-client/chromium-22.0.1229.79 multiple vulnerabilit...
- 437664** [RFC] <www-client/chromium-22.0.1229.92 multiple vulnerabilit...
- 437984** [RFC] <www-client/chromium-22.0.1229.94 SVG use-after-free and ...

The comments section shows three entries:

- #1 I like —Sean Amoss, Thu, 06 Sep 12 21:56
- #2 Is this also resolving CVE-2012-5376? —Sean Amoss, Sat, 13 Oct 12 20:53
- #3 Yes, CVE-2012-5376 is addressed in 22.0.1229.94, but it was not mentioned in the release notes. I've notified upstream about that, thanks for noticing! GLSA updated to also mention that. —Pawel Hajdan, Jr., Sat, 13 Oct 12 21:17

Administrative contact: security@gentoo.org

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
```

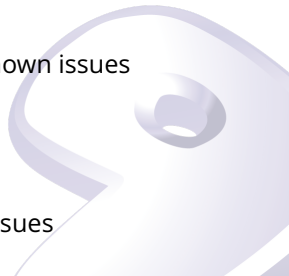
```
=====  
Synopsis: A vulnerability in mini_httpd could allow  
remote attackers to execute arbitrary code.
```

```
...
```

```
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
- 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
- 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

