Keeping Gentoo Secure

Open Source Security and how Gentoo does it

Alex Legler <a3li@gentoo.org>

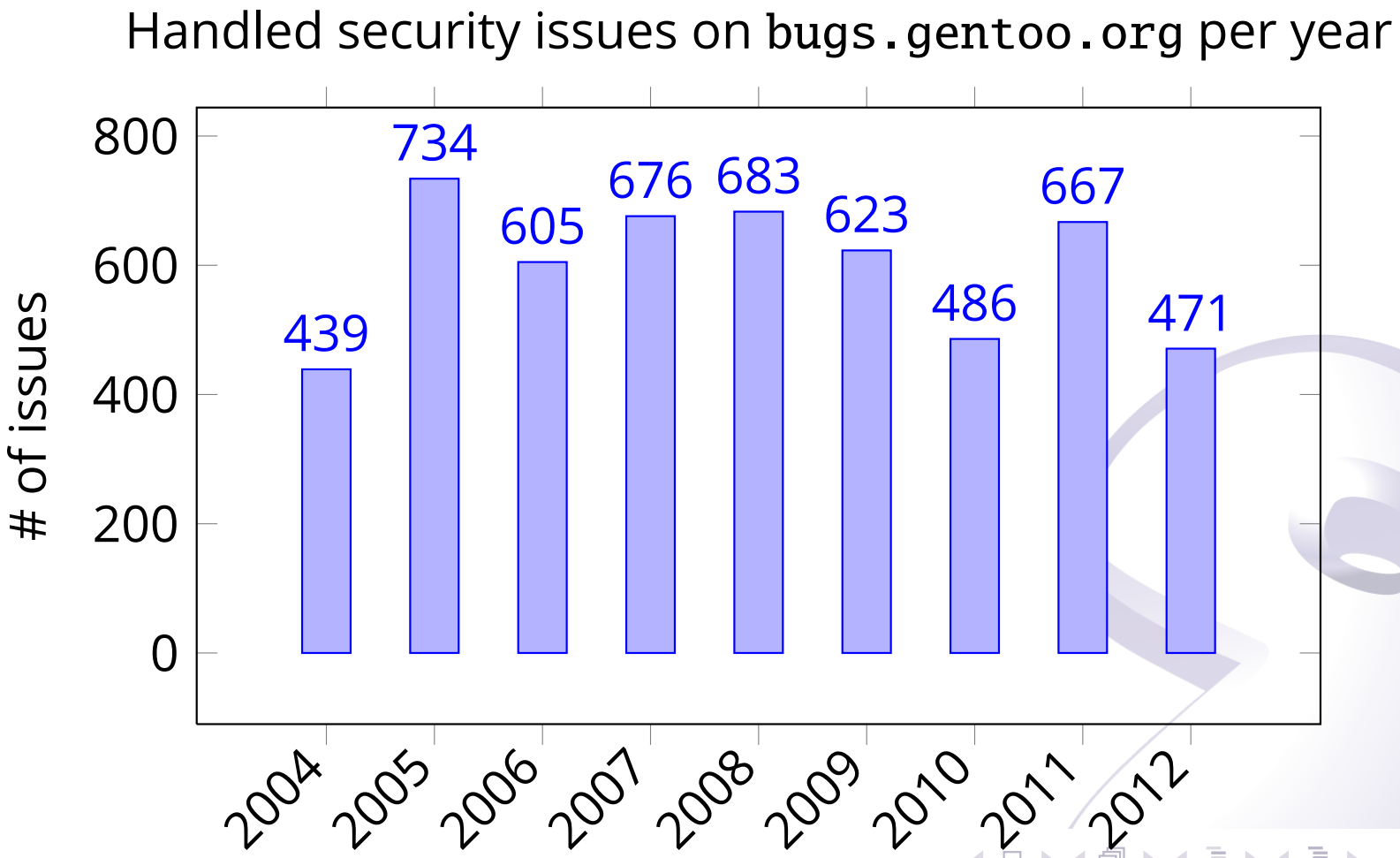
Gentoo Linux Security Team

Gentoo Miniconf Prague
October 2012

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?



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

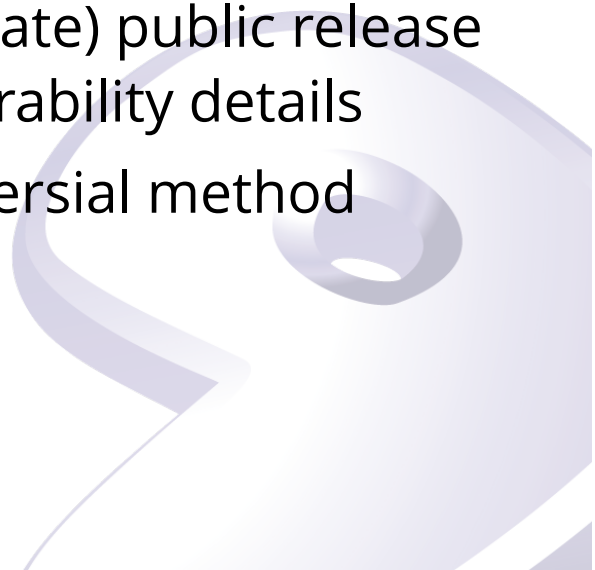
Vulnerability Disclosure Methods

Responsible disclosure

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

Full disclosure

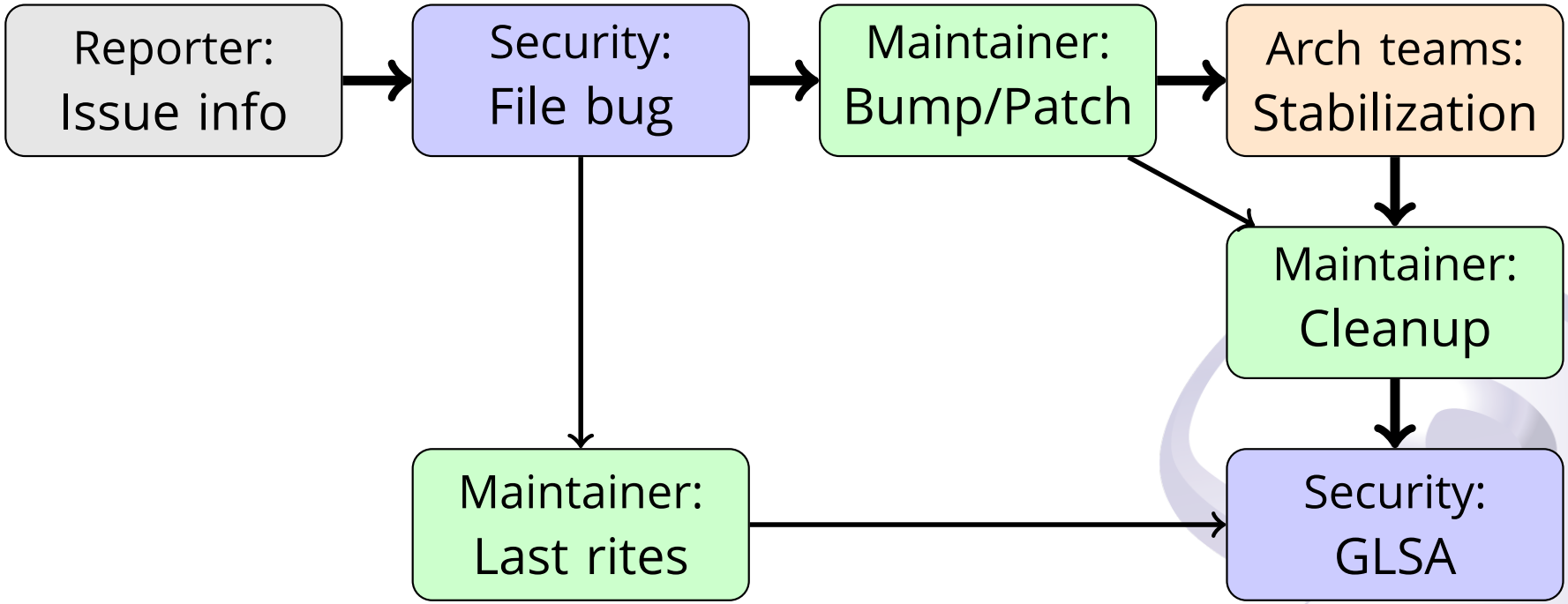
- (Immediate) public release of vulnerability details
- Controversial method



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**

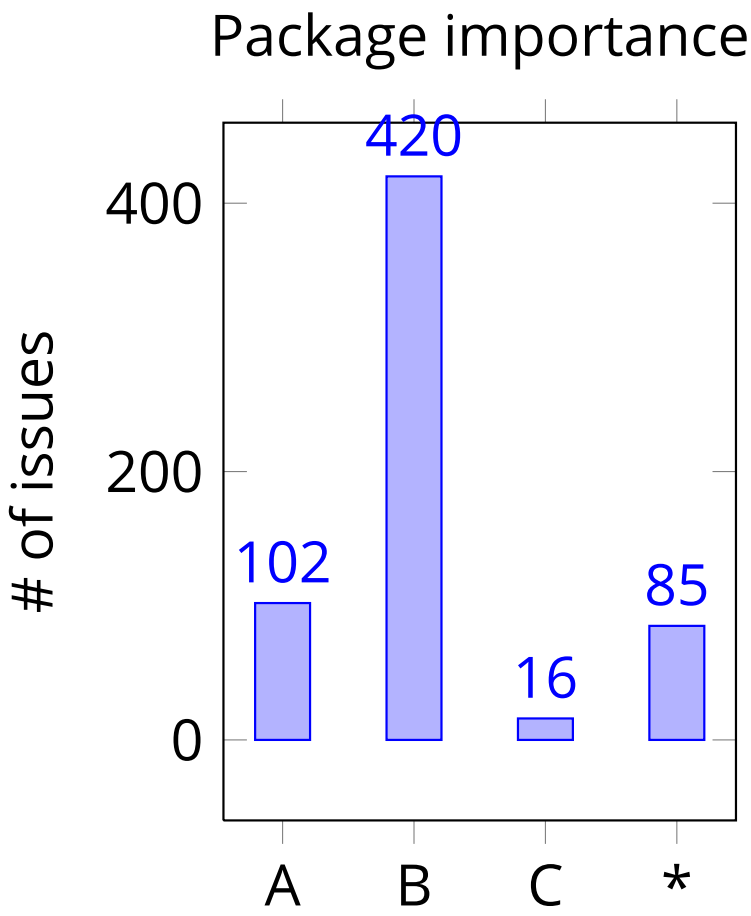
Workflow: Bug handling: Tracking status

Example status

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

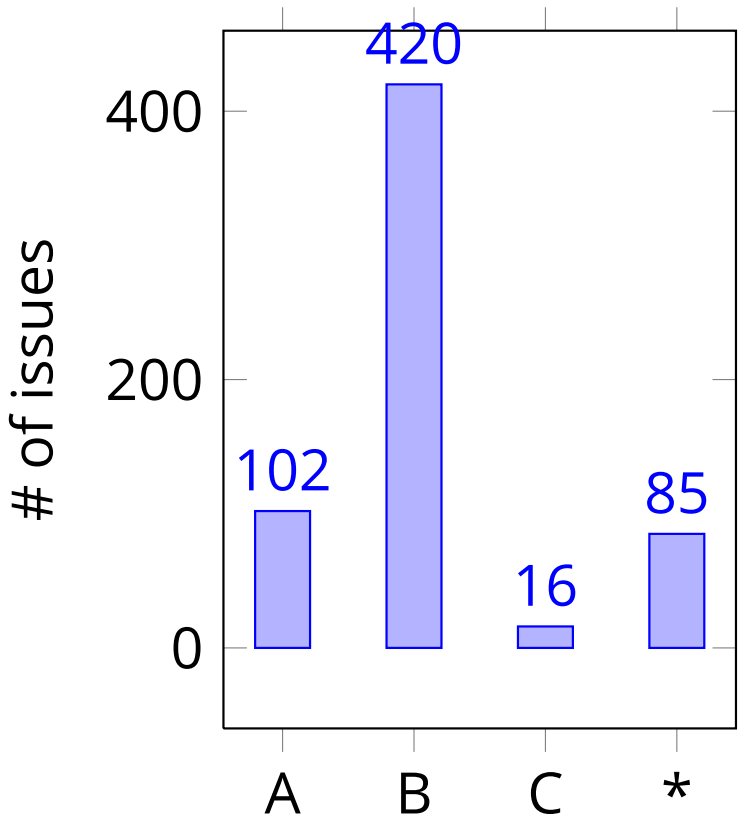
- `[upstream]`: Waiting for an upstream fix
- `[upstream/ebuild]`: Waiting or patching?
- `[ebuild]`: Updated ebuild pending
- `[stable]`: Stabilization is performed
- `[glsa?]`: Deciding whether to release a GLSA
- `[(no)glsa]`: (no) GLSA released

2011 issue statistics

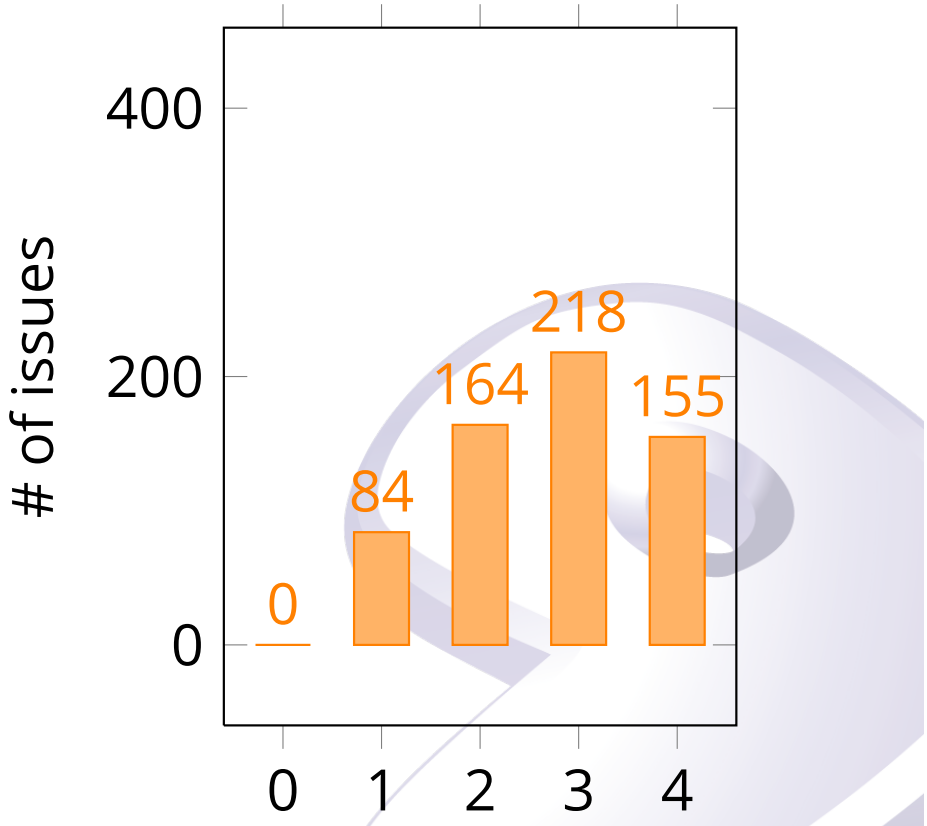


2011 issue statistics

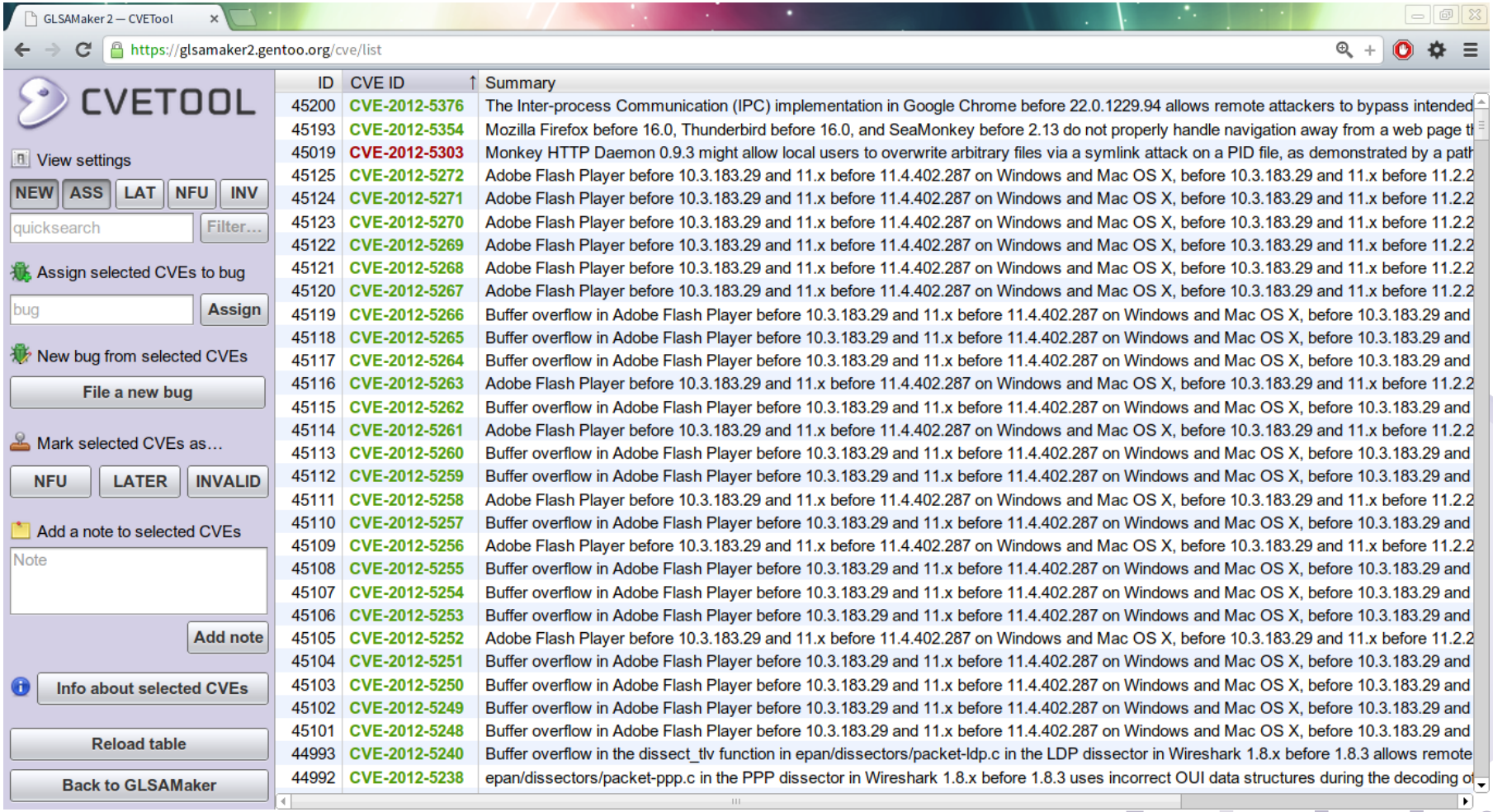
Package importance



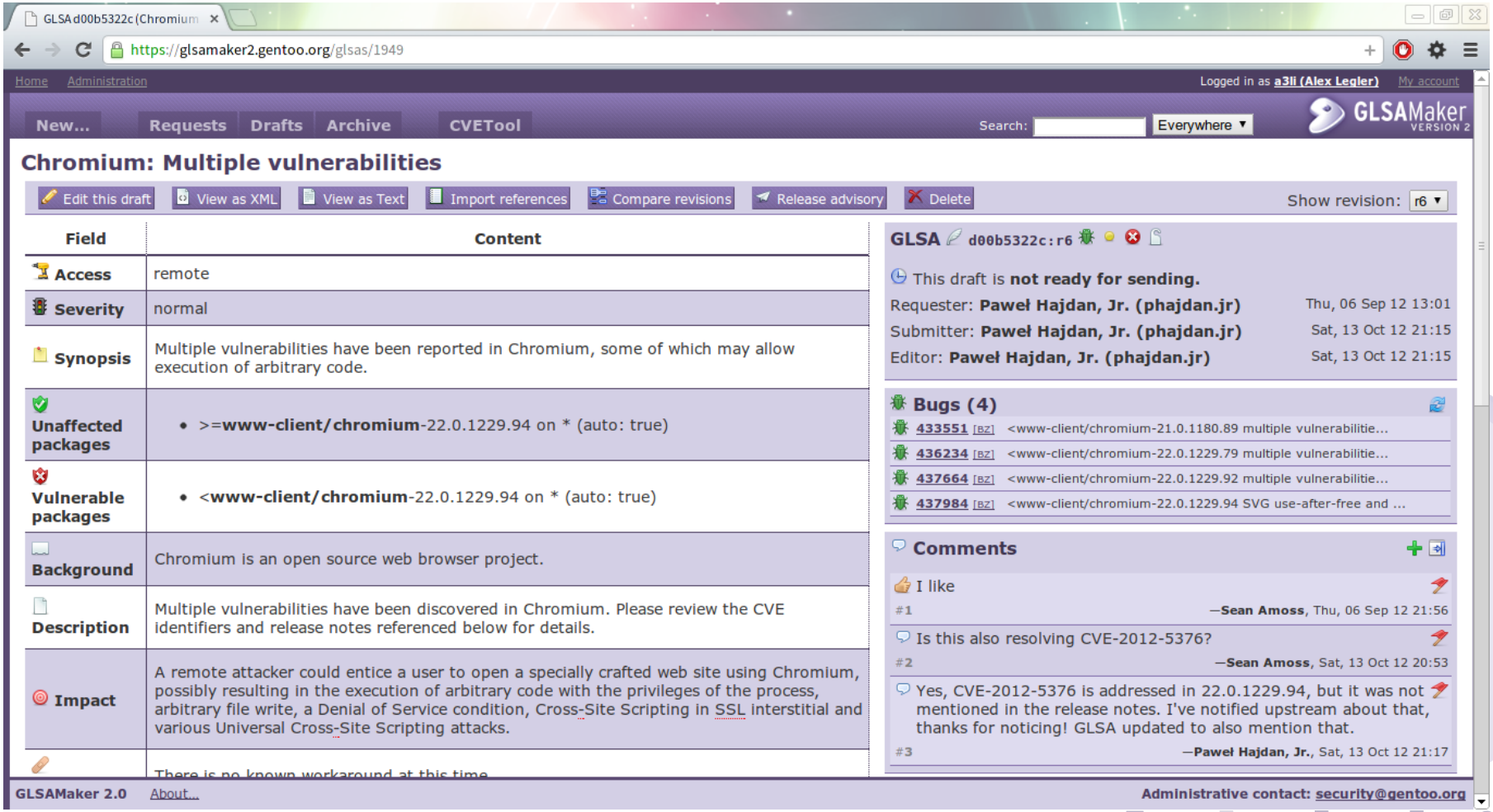
Issue severity



Tools: CVETool



Tools: GLSAMaker



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
```

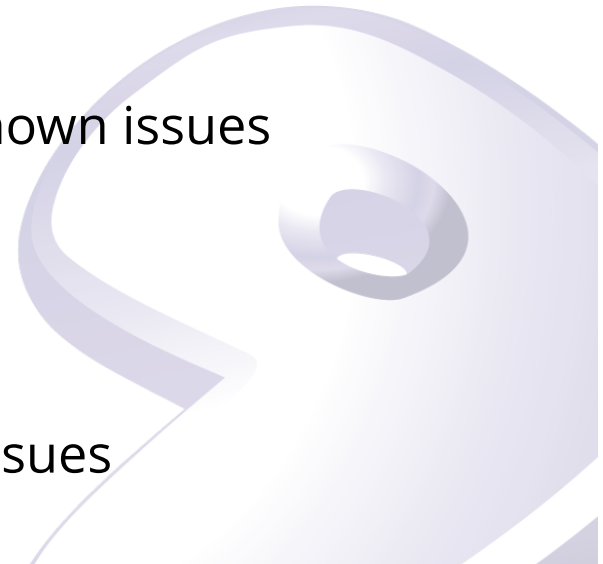
glsa-check (3)

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