Agenda

- Introducing the team
- Reactive Security
- Proactive Security
- Summary/Outlook
Who are we?

Johannes Segitz
Sr. Security Engineer
jsegitz@suse.com

Marcus Meissner
Sr. Projectmanager Security
meissner@suse.com
Introducing the team

**Teamlead**: Ivan Teblin

**Projectmanager**: Marcus Meissner

**Certifications Projectmanager**: Katia Rojas

**Security Engineers**:
- Alexander Bergmann
- Alexandros Toptsoglou
- Hans Löhr
- Johannes Segitz
- Malte Kraus
- Matthias Gerstner
- Robert Frohl
- Wolfgang Frisch

**Open Positions**: 1 Reactive Engineer, 1 Proactive Engineer
Reactive vs Proactive

**Reactive:**
- Incident handling
- Marcus, Alexander, Alexandros, Robert, Wolfgang

**Proactive:**
- Audit programs and system services (systemd, dbus, network)
- Approve product releases
- All security work before shipment
- Johannes, Malte, Matthias, Hans
Reactive Security
Reactive Security

- Reacting on reported security issues
- Roles:
  - Incident Managers
  - Update Manager
- Coordinating from begin to end, delegate
  - Fixing to package maintainer
  - Source review to OBS/IBS reviewers
  - Testing to QA
- Release the update
- Documentation
  - Human and machine readable
Incidents

Open bug
- Summary line: VUL-[012]: CVE: package: summary
- Description with references / links
- Patches and reproducers attached
- Assign to packager / bugowner

SMASH issue
- Simplified rating and CVSSv3 scoring
- Assign affected Software (for SUSE Linux Enterprise family)
- Planning Update or Starting Update immediately
Opened bugs per week: 2006 – 2020
SMASH Ticket System

<table>
<thead>
<tr>
<th>Name</th>
<th>Rating</th>
<th>Flags</th>
<th>Issue Summary</th>
<th>Packages</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>bnc#1136184</td>
<td>moderate</td>
<td></td>
<td>python-botocore needs to support urllib 1.25 for CVE-2019-9947</td>
<td></td>
<td>Not For Us, Analyze</td>
</tr>
</tbody>
</table>

Showing 1 to 2 of 2 entries

Served by SMASH 3.3.27. Please report bugs or feature requests to GitLab, check documentation for help and see status page for status overview.
<table>
<thead>
<tr>
<th>Name</th>
<th>Owner</th>
<th>Rating</th>
<th>Flags</th>
<th>Issue Summary</th>
<th>Packages</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>bnc#1133375</td>
<td>meissner</td>
<td>important</td>
<td>⬜️</td>
<td>VUL-1: CVE-2019-9928: gstreamer-0_10.gstreamer: GStreamer before 1.16.0 has a heap-based buffer overflow in the RTSP connection parser via a crafted response from a server, potentially allowing remote code execution.</td>
<td>gstreamer-0_10.gstreamer</td>
<td>Not For Us</td>
</tr>
<tr>
<td>rhd#1705414</td>
<td>abergmann</td>
<td>moderate</td>
<td>☼</td>
<td>CVE-2019-11598 ImageMagick: heap-based buffer over-read in the function WritePNMImage of coders/pnm.c leading to DoS or information disclosure.</td>
<td>ImageMagick</td>
<td>Not For Us</td>
</tr>
<tr>
<td>bnc#1118212</td>
<td>meissner</td>
<td>important</td>
<td>⬜️</td>
<td>VUL-0: kernel-source: Misbehaving SATA device leaks kernel memory pages to unprivileged user.</td>
<td>kernel-source</td>
<td>Not For Us</td>
</tr>
<tr>
<td>bnc#1136183</td>
<td>meissner</td>
<td>moderate</td>
<td>☼</td>
<td>VUL-1: ImageMagick: PCL might still decode using ghostscript.</td>
<td>ImageMagick</td>
<td>Not For Us</td>
</tr>
<tr>
<td>rhd#1705406</td>
<td>abergmann</td>
<td>moderate</td>
<td>☼</td>
<td>CVE-2019-11597 ImageMagick: heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c leading to DoS or information disclosure.</td>
<td>ImageMagick</td>
<td>Not For Us</td>
</tr>
<tr>
<td>bnc#1126064</td>
<td>meissner</td>
<td>moderate</td>
<td>☼</td>
<td>VUL-0: freetype2: information leakage due to rendering time differences.</td>
<td>freetype2</td>
<td>Not For Us</td>
</tr>
<tr>
<td>bnc#11085255</td>
<td>meissner</td>
<td>moderate</td>
<td>☼</td>
<td>VUL-1: avahi: remote denial of service (out of memory abort) crashes.</td>
<td>avahi</td>
<td>Not For Us</td>
</tr>
<tr>
<td>bnc#1132190</td>
<td>meissner</td>
<td>moderate</td>
<td>☼</td>
<td>VUL-0: kernel-source: kernel oops through malicious USB camera devices.</td>
<td>kernel-source</td>
<td>Not For Us</td>
</tr>
<tr>
<td>bnc#1131221</td>
<td>meissner</td>
<td>moderate</td>
<td>☼</td>
<td>VUL-1: CVE-2018-3979: x186-video-nouveau: A remote denial-of-service vulnerability.</td>
<td>x186-video-nouveau</td>
<td>Not For Us</td>
</tr>
</tbody>
</table>
Update submissions

Packager submits updates

Security Team
• Writes metadata (summary, description, issues)
• Checks if building
• Pushes to QA

QA tests update
• Automated and manual testing

Security Team
• Releases update
• Additional documentation work
## Maintenance incidents on QA (138):

Showing 1 to 138 of 138 entries

<table>
<thead>
<tr>
<th>ID</th>
<th>RR</th>
<th>Created</th>
<th>Deadline</th>
<th>Prio</th>
<th>Test</th>
<th>Rating</th>
<th>Packages</th>
<th>QA</th>
<th>Issues</th>
<th>Search:</th>
</tr>
</thead>
</table>
| 7396| 164800 | 2018-05-11| 2018-05-18| 515  | ⚤    | moderate | ardana-ansible  
ardana-barcisan  
ardana-cassandra | [cloud-qe] | ⚫ 23 bugs | HPE- Helion-  
        OpenStack-8  
        OpenStack-Cloud-8 |
| 6195| 148024 | 2017-12-02| 2018-01-01| 480  | ⚤    | moderate | bzip2  | rommel | ⚫      | DEBUGINFO-11-SP3-TERADATA  
        SERVER-11-SP3-TERADATA |
| 7432| 165005 | 2018-05-15| 2018-05-22| 468  | ⚤    | important | aaa_base | ⚫ ⚫ junguo.wang | bsc#1088524 | OpenStack-Cloud-7  
        OpenStack-Cloud- 
        Magnum-Orchestration-7  
        POS-12-SP2-CLIENT  
        SAP-12-SP2  
        SERVER-12-SP2  
        STORAGE-4 |
Reactive work – what is delivered

The updates themselves!

Notifications for every update

- Web https://www.suse.com/support/update/
- E-Mails to sle-security-updates@lists.suse.com, sle-updates@lists.suse.com and opensuse-security-announce@opensuse.org

Autogenerated information:

- CVE webpages https://www.suse.com/security/cve/
- OVAL data https://www.suse.com/support/security/oval/
Some statistics for 2019

- CVEs processed: 2496 (2732 in 2018)
- Bugs opened: 2079 (2284)
  - 306 (140) Linux Kernel
- Security updates released:
  - 1335 (compared to 1499) for SLE
  - 952 (978) for openSUSE (562 (328) SLE imports) (around 59%)
- CVEs fixed: 2314 (previous 2386)
  - 1775 openSUSE
  - 1830 SLE
Proactive Security
Proactive Security Tasks

Making products as secure as possible before shipment

Primary tool: Our zoo of bots and automated checks during build/submission (mainly rpmlint):

- Non-default permissions (e.g. setuid/setgid/capabilities)
- DBUS services
- PolicyKit rules
- PAM modules
- Cronjobs
- Dangerous constructs in the packaging (e.g. %post/%pre, rpmlint suppression)
Proactive Security Tasks

Massive improvements in the last two years in this area:
• Added many additional vectors to be considered
• Whitelist content, not just filepaths
• Check for devices
• Have whitelists unique to each codestream (ongoing)
• Improved process of maintaining whitelists (github as primary source)
• Improved visibility in the tricky rpmlint(-mini) setup in our products
• Vary badness of warnings between home projects and products

Matthias Gerstner was the driving force behind a lot of this
Proactive Security Tasks

Example for a message you might see during build

```
[ 131s] ppc64-diag.ppc: E: cronjob-unauthorized-file (Badness: 10) /etc/cron.daily/run_diag_encl
[ 131s] A cron job file is installed by this package. If the package is
[ 131s] intended for inclusion in any SUSE product please open a bug report to request
[ 131s] review of the package by the security team. Please refer to
[ 131s] https://en.opensuse.org/openSUSE:Package_security_guidelines#audit_bugs for
[ 131s] more information
```

Please talk to us as soon as possible. We’re swamped and need to prioritize

For products higher badness values will prevent your package from building
Proactive Security Tasks

Additionally:

• Reviewing/add new compiler hardening flags
• Review and audit of new components
• Whatever comes up, e.g. review changes in OBS
• More recently: Code reviews for daemons listening on the network. E.g. Matthias’ awesome work on kdeconnectd
How we work

Security audits are “rolling”
• Based on openSUSE Factory development
• Based on packages
• But also on final product

Most of our work for SUSE is done in openSUSE Factory!
113 new AUDIT-0 bugs in 2019 (74 in 2018)
Challenges

- Not enough hours in the day ;)
- Competing demands, missing granularity/user decision in existing mechanisms (e.g. polkit profiles)
- Old technology used by customers (e.g. missing open flags), mostly doesn’t concern openSUSE
Roadmap

• Extend coverage to new products/containers. CaaSP and CAP are still a problem for us as they fall out of our usual processes
• Embed engineers into product teams/foster security champions
• Renew efforts around AppArmor, maybe SELinux
• CFI
• More automation & more manpower
Where the community can help

- Tracking works mostly fine and is difficult to work with the community due to private security disclosures.
- We always need help with fixing issues that we track. This is a good way to learn more about security.
- As AppArmor is the technology used for openSUSE: Additional profiles/improve existing.