10 years of X.Org security list

Matthieu Herrb

XDC 2021 - september 16

About myself

- 58 years old, Research Engineer at CNRS in Toulouse, France
- X.Org is a hobby, not in my main job.
- Maintainer of X.Org on OpenBSD (project Xenocara)
- Started with XFree86 in 1999, moved over to X.Org
- Been with `xorg-security` with Alan Coopersmith since 2008

Introduction

Handling of security issues reported to X.Org via `xorg-security@lists.x.org`

Not necessarily representative of the security of the X server / libraries / applications in a whole.

$\rightarrow$ this is not a general talk about the (in)security of X.

Responsible Vulnerability disclosure

Vulnerabilities in widely used software can have a huge bad impact on existing installations.

General process, globally agreed on by many Free and Open Source projects.

- "White hats" security researchers report the vulnerabilities they find privately, work with the maintainers on a fix and decide on a disclosure date.
- Gives time for binary package maintainers to prepare updates, ready to be installed.
- So this is a limitation to full transparency, to mitigate the impact (avoid "zero days").
- But we should keep the embargo on vulnerabilities as short as possible.
- Some organizations (not X.Org!) have bug bounties programs to encourage this process.

Full disclosure

Vulnerabilities are disclosed as soon as they are found by researchers

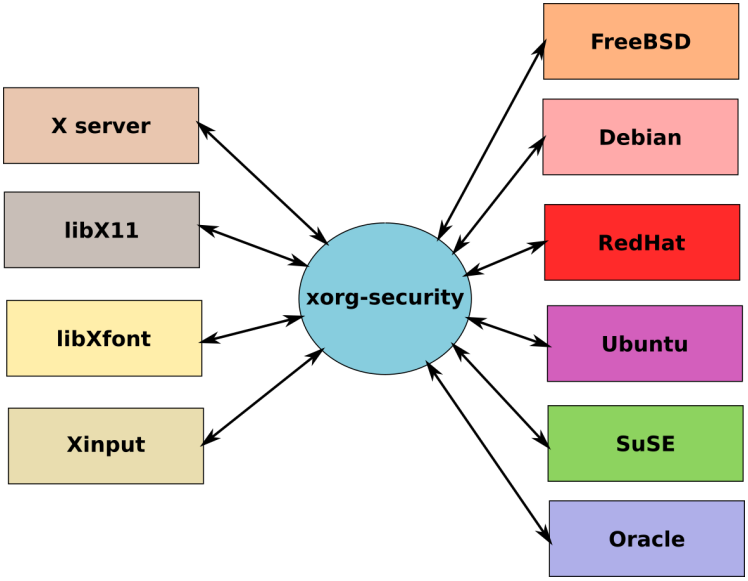
Patches are not yet available

Users get exposed to the vulnerability.

Note that this can happen, even with a responsible disclosure policy in place:

- because of “black hats” who don’t follow the policy
- because of mistakes from developers who don’t see the security implications of their bug fixes (or don’t know about the policy)

Interactions



External Actors and vocabulary

- MITRE and CVE-IDs
- CVE Numbering authorities (CNA)
- The OSS-security mailing list and the associated wiki
- The distros mailing-list
- US-CERT and other CERTs
- ...

An example of the actual process

2019-03-06 jolibug@gmail.com sends an email to `xorg-security@lists.x.org` talking about a new vulnerability discovered in libXfoo version 3.33.

2019-03-07 some-dev@example.com, member of the list, confirms the existence of the problem and analyzes that it was introduced by a change in version 2.45. They answer to jolibug to acknowledge their email and asks them if a CVE-Id has already been allocated or a disclosure date has been decided. They also propose a patch.

2019-03-08 jolibug answers that no date
has been set up and no id was allocated.
they're willing to postpone the disclosure
of the bug up to a reasonable delay.

2019-03-08 some-dev asks Redhat for a CVE-Id

2019-03-09 someone from Red-Hat allocates CVE-2019-666 for this.

2019-03-09 knowing that libXfoo is used by a number of Linux and BSD distros, some-dev writes to the distros mailing list, and proposing 2019-03-22 (14 days later) as release date.

2019-03-09 another-dev@BlueCap.com answers to the distros mail signaling the proposed date is a friday, which is a bad day for releasing security advisory and suggests to move it forward to 2019-03-19.

2019-03-09 some-dev agrees and informs jolibug and xorg-security.

2019-03-11 eric@nobugs.com says in an email to distros and xorg-security that some-dev's patch isn't fully solving the issue: a similar issue exists in another function in libXfoo.

2019-03-12 new version of the patch sent to xorg-security, jolibug and distros.

2019-03-14 some-dev sends xorg-security and jolibug an draft of the security advisory, what should be the final patch.

2019-03-15 some-dev prepares a new release of libXfoo including the patch and checks that it's good for release.

2019-03-19 14:00 GMT

- libXfoo 3.34 is released
- the security advisory is sent to `xorg-announce@lists.x.org` and `oss-security@lists.openwall.com`
- the X.Org wiki security page is updated
- jolibug send out their advisory to various security mailing lists and social networks.

shortly after: The bug is now public !:

- Various distros distribute updated binary packages.
- MITRE makes the CVE-ID description public,
- Various CERTS, as well as LWN and Phoronix publish their own news on the bug,

A Quick Taxonomy of the reported vulnerabilities

In the early days trivial buffer overflows, argument sanitizing bugs,..
almost always direct local root access.

nowadays Mostly protocol handling bugs

- both client side and server side
- insufficient or incorrect validation of the (complex) protocol messages $\rightarrow$ unauthorized memory accesses
- some file format decoding bugs (mostly fonts)

Mitigations :

- less privileges for the X server
- less privileged X clients
- XCB automates protocol encoding/decoding, but not done server side yet.

Current state / Conclusion

- Need new people
- Old code base knowledge is fading away...
- Not reactive enough
- How to get CVE IDs ? (stay with RedHat or become a CNA?)
- Process integration in Gitlab:
  - management of private issues / merge requests
  - management of the access to previous (per repository/project...)
- Lack of involvements of vendors (general issue):
  - patches reviews
  - helping with code improvements ?
- **BoF session on friday 14:30 - 16:60**

Resources

- the Security Checklist on the X.Org wiki (to be revised)
- Security process for Open Source Projects, Alex Gaynor, 2013
- The CERT Guide to Coordinated Vulnerability Disclosure
- The OSS-security mailing list and wiki
- The distros mailing-list
- The CVE request form at MITRE

Questions ?