black hat
EUROPE 2023

DECEMBER 4-7

EXCEL LONDON / UK

black hat EUROPE 2023

Through the Looking Glass:

How Open Source Projects See Vulnerability Disclosure

ECLIPSE FOUNDATION

Marta Rybczynska

Disclaimer

Stories included in this talk are based on facts, but have been heavily changed for illustrative purposes.

Any resemblance to actual events or persons, living or dead, is entirely coincidental.

Have you contributed to an Open Source project?

Have you submitted a potential vulnerability report to an Open Source project?

Have you had a vulnerability confirmed by an Open Source Project?

Who is Marta?

Involved in Open Source projects for the last 20+ years. Contributed to a varied set of projects from the Linux kernel to the KDE environment.

Currently helping projects at Eclipse Foundation in **communicating with security researchers** on vulnerability reports, among other things.

PhD in Telecommunications, focus on networking and anonymity systems.

Some possible responses

1. Thanks, this will be fixed in X.y
2. This is not a security issue.
3. You say this is a potential issue, have you tested to see if it works?
4. If you care, submit a fix.
5. We do not issue CVEs.

When does each of them happen?

Thanks, this will be fixed in X.y

Thanks, this will be fixed in X.y

- Well-written report
- Contains all information needed to reproduce
- Often a obvious bug (crash)

This is not a security issue

This is not a security issue

- Not a remote code execution without user's action
- Development team lacking training
- A project that has never received a vulnerability report
    - Or it happened long time ago
- An issue in a tool expected to be used locally only
- Report from the researcher not understood
- … or just no issue

You say this is a security issue. Have you tested to see if it works?

You say this is a security issue. Have you tested to see if it works?

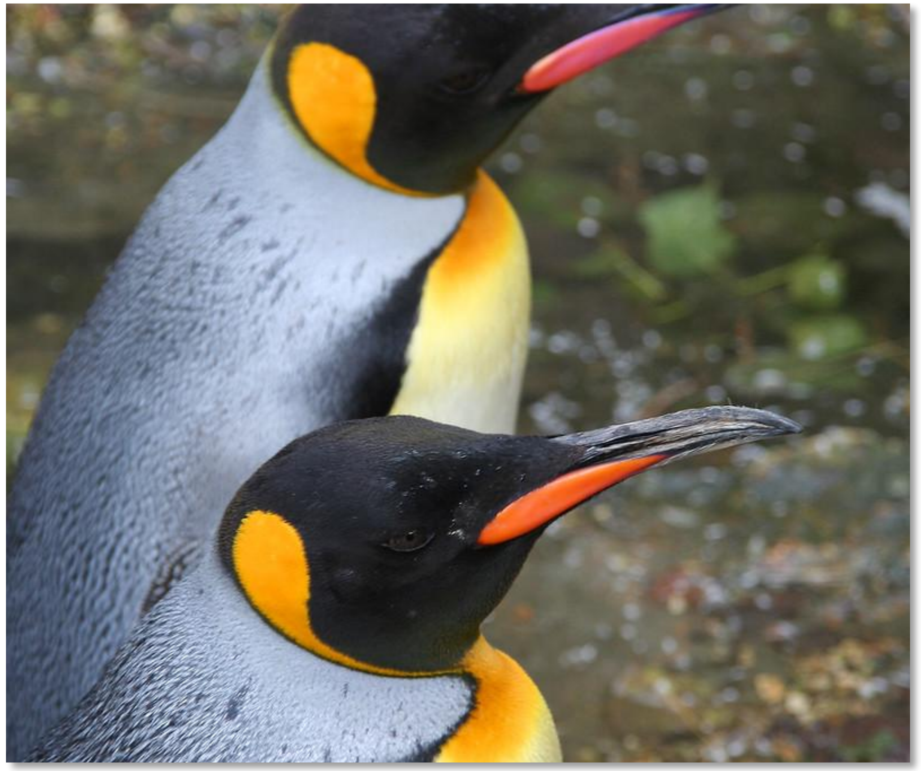
- A “potential” vulnerability, happening in rare/theoretical situation
- Looks like a false positive from a fuzzer
- The notification is vague/unclear/generic
- The notification is missing a clear reproducing procedure

If you care, submit a fix

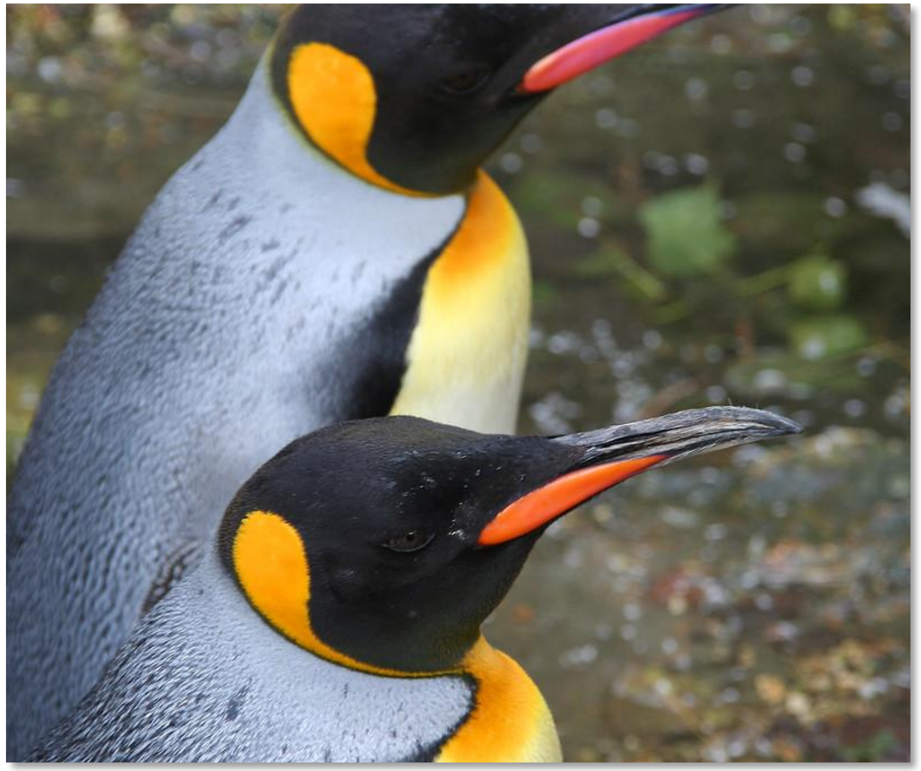
If you care, submit a fix

- Not an “obvious” bug
- Rarely used component, possibly unmaintained
- Understaffed project team, lack of maintenance funding
- A project that has never received a vulnerability report
    - Or it happened long time ago

We do not issue CVEs



We do not issue CVEs



- A report submitted to the Linux kernel
- Overworked maintainers

What you should know about Open Source

What you should know about Open Source

1. Projects vary by scope, experience…
2. Developers often lack security education
3. Maintenance is an unsolved problem
   - Funding often goes to new features
   - Maintainers (ALSO in big projects) often contribute on their own time

What have we done at Eclipse Foundation

What have we done at Eclipse Foundation

1. Migrated security reporting from Bugzilla to GitLab/GitHub
2. Promote SECURITY.md
3. Regular trainings for developers
4. Tooling for repository management
5. Security team offers advice
   - “Translation”
   - Helping with CVE record filling etc

Recommendations

Recommendations for security researchers

1. Write clear vulnerability reports
   - What is the issue, why important (attack scenarios!)
   - How to reproduce
2. Avoid dialect (security abbreviations)
3. Avoid half-baked issues from automatic tools
4. Spend 5 minutes to find the recommended way to contact the project
5. If you are a teacher: verify your student’s reports

black hat®
EUROPE 2023

Through the Looking Glass:
How Open Source Projects See Vulnerability Disclosure

ECLIPSE®
FOUNDATION

Marta Rybczynska

Image credits

1. "Fireworks" by pga_99 https://www.flickr.com/photos/155831598@N06/ Public domain https://flic.kr/p/VFN3Ay
2. sign-1438603 by Mike Goad https://www.flickr.com/photos/exit78/ Public domain https://flic.kr/p/L2F6oU
3. "The Maze" by Peter Hurford https://www.flickr.com/photos/peterhurford/ Public domain https://flic.kr/p/5WFQTL
4. "Untitled" by Anneke https://www.flickr.com/photos/demolen/ Public domain https://flic.kr/p/2oFaNpn
5. “Emperor Penguins” by Lark Ascending https://www.flickr.com/photos/vwilliams/ Public domain https://flic.kr/p/6V7h3w