Security Process

Alex Gaynor

Background

- Software engineer at Rackspace
- PSF director
- Core developer of Django, CPython, PyPy, etc.
- Developer of PyCA Cryptography, PSRT member, Twisted security contact

Why do we care?

Why are security bugs special?

Agenda:

How to deal with reports.

First touch

/security/

- Description of the process
- PGP public key for security@
- Responsible disclosure policy

Sign in

slack

Policy

Review our statement on **Security & Confidentiality**.

To report a security vulnerability, please email **security@slack.com**

Reporting Security Vulnerabilities

This page is intended for security researchers. To find out more about Slack's security, please visit our security information page.

If you believe you have found a security vulnerability on Slack, we encourage you to let us know right away. We will investigate all legitimate reports and do our best to quickly fix the problem.

Please **submit your report on HackerOne** and our security team will respond as soon as possible.

Responsible Disclosure Policy

If you give us a reasonable time to respond to your report before making any information public and make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our service during your

Upon contact

Fix the bug

Shipping it

- Get a CVE number
  - distros@
  - oss-security@
    - MITRE
- Coordinate with re-distributors
- Issuing the release

Release announcement

- A precise and complete description of the issue
- CVE number
- The release artifact itself
- Raw patches
- Credit to the reporter

0 Days

Summary

- Getting reports
- Developing patches
- Coordinating with down streams
- Issuing releases

Common Mistakes

- Incomplete disclosure
- Bad coordination
- Zero Days

Pre-notification

Pre-notification requirements

- Clear security contact
- Description of how information will be used
- Large or otherwise high visibility

Bounties

HackerOne and BugCrowd

Security Impact Ratings

Wrapping Up

- Add a /security/ page and security@ address
- Document how vulnerabilities will be handled
- Consider creating a bounty program

3 things to check for

- Good password storage algorithm
- HTTPS certificate and hostname verification
- SQL injection

Thanks

alex.gaynor@gmail.com

alexgaynor.net