How secure is Open Source code?

Maria Emilia Torino
emilia.torino@canonical.com
@emi_torino
is the open source code more secure
is open source software more secure than proprietary products
is open source software more vulnerable

Google Search  I'm Feeling Lucky
Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver’s license numbers.

The attack on the company represents one of the largest risks to personally sensitive information in recent years, and is the third major cybersecurity threat for the agency since 2015.

Equifax, based in Atlanta, is a particularly tempting target for hackers. If identity thieves wanted to hit one place to grab all the data needed to do the most damage, they would go straight to one of the three major credit reporting agencies.

“This is about as bad as it gets,” said Pamela Dixon, executive director of the World Privacy Forum, a nonprofit research group.
How secure is Open Source code?
“@Canonical Security is at the heart of Ubuntu”

https://ubuntu.com/security
“The UK Government puts Ubuntu in first place for security”

What is Canonical/Ubuntu doing to lead open source security?
#1 Secure out of the box

- Threat modeling
- Automated code inspection
- Secure code guidelines
- Security Testing
- Security code reviews
#1.1 Secure Code Guidelines

- Do not trust input
- Sanitize output
- Do not reinvent the wheel
- Minimize the attack surface
- Design for least privilege
- Apply defense in depth
- Do not rely on security by obscurity
- Do not ignore compiler / toolchain warning messages
- Fail securely
- Encrypt network communications
- Test security
- Learn from mistakes

https://wiki.ubuntu.com/SecurityTeam/FAQ#Design
#1.2 Threat Modeling - STRIDE

- Spoofing - Authentication
- Tampering - Integrity
- Repudiation - Non repudiability

- Elevation of privileges - Authorization
- Denial Of Service - Availability
- Information disclosure - Confidentiality

https://en.wikipedia.org/wiki/STRIDE_(security)
#2 Secure by process

Fix & validation

Triage

Publish

https://cve.mitre.org/
https://usn.ubuntu.com/
#3 Certified compliance

Federal Information Processing Standard (FIPS) 140-2 Level 1

Common Criteria EAL2 (ISO/IEC IS 15408)

Security Technical Implementation Guide (STIG)

Center for Internet Security (CIS) benchmark

https://ubuntu.com/blog/canonicals-security-certifications
#4 Communication & Collaboration

#ubuntu-hardened on Freenode IRC

https://ubuntusecuritypodcast.org/

security@ubuntu.com

@ubuntu_sec on Twitter
There is no secret sauce, but...

- A culture of Security *first*
- A dedicated team seen as a partner
- A set of processes in place
- A set of tools supporting processes
- A great team of smart and experienced people
- A supporting structure for helping everybody to grow
Get Involved!

https://wiki.ubuntu.com/SecurityTeam/GettingInvolved
https://ubuntu.com/community
https://canonical.com/careers
Thank you. Questions?
https://www.zdnet.com/article/critical-linux-security-hole-found/
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
https://fortune.com/longform/sony-hack-part-1/
https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html
https://atmanco.com/blog/hiring/recruitment-questions-to-ask-when-hiring/