Securing Software from the Supply Side

Nickolas Means
Senior Engineering Manager, Security and Compliance
GitHub
Open Source
99% of software projects use open source
Security Researchers

- **Identify**
- **Disclose**

- Manual discovery
- Private disclosure
Security Researchers

- Identify
- Disclose

Maintainers

- Fix
- Alert

- Manual discovery
- Private disclosure
- Can’t collaborate in private
- Notifying all users
Security Researchers

- Identify
  - Manual discovery
  - Private disclosure

- Disclose

Maintainers

- Fix
  - Can’t collaborate in private
  - Notifying all users

- Alert

Developers

- Update
  - Updates aren’t applied

- Prevent
  - Vulnerabilities recur
Demo
Update
Prevent
Developers
Fix
Alert
Maintainers
Identify
Disclose
Security Researchers
Manual discovery
Coordinated disclosure
Vulnerabilities recur
Alert all users
Collaborate privately
Automatic security updates
Securing Software from the Supply Side

Nickolas Means
Senior Engineering Manager, Security and Compliance
GitHub