The State of Third-Party Software Security in 2020

Omar Santos
os@cisco.com
This presentation is dedicated to CRob
Agenda

- Introduction to third-party software (commercial and open source) security challenges.
- Third-party software (TPS) security tools.
- PSIRT’s role in TPS security.
- Disclosing TPS vulnerabilities.
- TPS security in the cloud.
Who invited this guy?

Are you *#$^& kidding me?
Active Discussion

WHO CAME UP WITH THE TERM “BIRDS OF A FEATHER”?
TPS Security...
It’s 2020... Are we better than we were 10 years ago?
SLOs/SLAs in Contracts (Customer Contracts and Supplier Contracts)
Fixing Open Source is not one company’s task...
Hackers are going after Cisco RV320/RV325 routers using a new exploit

Attacks on Cisco routers started hours after the publication of proof-of-concept code on GitHub.
Seriously? Cisco put Huawei X.509 certificates and keys into its own switches

How did cryptographic certificates and keys issued to Huawei end up in Cisco gear?
ODMs (Contracts, SLOs/SLAs, Testing, SDLC, etc. etc...)
TPS and the Cloud...
What about Disclosures?
Cloud Solutions

Powering the multicloud world.

Watch video (0:52)
Technology

Cisco Enters Chip Market, Supplying Microsoft, Facebook
Cisco Silicon One

Meet the first unified silicon architecture for web scale and service provider networks.
Policy creation and enforcement
Some require IDE support
Build infrastructure
Reporting
Language support
Container Decomposition
Performance
BMC/ILOs & Connected Power Supplies
Automated Vulnerability Disclosures
5000 CVEs per year

x 700 products (we have thousands of registered “projects” (a project can be a new major release or a new product)).

If 10% of them affect a product...
500 x 700 = 350,000 notifications / bugs

That’s 958 potential disclosures per day. Even if you consolidate, there could be over 1,000 per week!
So...
Automated Vulnerability Disclosures...
Triage?
CVSS from NVD?
Does it work for automation?
What if you develop Open Source? How do you disclose?
Thank you!