Mature PSIRTs Need Mature Tools

Beverly Finch | beverlyfinch@lenovo.com
PSIRT Program Manager, Product Security Office
Lenovo USA, Morrisville, North Carolina
Bio: Beverly Finch

PSIRT Program Manager

- Executive Project Manager (20+ years PMI Certified)
- Lean Six Sigma
- Launched Lenovo PSIRT, 2014
- MITRE CVE Board
- FIRST.org Member
- FIRST PSIRT Framework Working Group
- Chair, Vendor SIG
Product Security Incident Response Team (PSIRT)

**Milestones**

- 2014: Established, permanently staffed
- 2015: Admitted to FIRST
  - Sponsored by Cisco, Intel
- 2016: CVE Numbering Authority

**Objectives**

- Respond to product vulnerability reports
- Coordinate with business units and industry to ensure clear direction and communication
- Negotiate disclosure timelines and plans with researchers and coordination centers
- Drive remediation
- Support customers by publishing product security advisories
- Engage with external PSIRTs to establish and promote best practices around security vulnerability handling

**Resource:**

- **Contact:** psirt@lenovo.com
- **Advisories:** https://support.lenovo.com/us/en/product_security/home
# Lenovo PSIRT Evolution

## Past
2014
- Reactive only
- Spreadsheet Tracking
- Security advisory control outside PSIRT

## Now
2015-2018
- Proactive
- Jira-based tracking tool
- Spreadsheet tracking of product attributes
- Security advisory publishing control
- Communications/Legal engagement
- SLA Dashboards
- Automated customer notification

## Future
2018+
- Product Attribute Database (PAD)
- PAD driven by composition analysis tools
- Increased ownership by brands
- Improved Security Advisories
- Add open source advisories
- Automated SLA Dashboards
Tooling Concerns

What products do we support?
What is included in our products?
What open source do we use?
Targeted case assignment
Advisory preparation
SLA Tracking
Customer notification
Current – Creating a Case

Sub-Tasks

1. Test - Lenovo Desktop BIOS/UEFI
2. Test - Lenovo Desktop - Drivers / Other Firmware task
3. Test - Lenovo Desktop - ME/AMT task
4. Test - Lenovo Notebook - BIOS/UEFI task.
5. Test - Lenovo Notebook - Drivers / Other Firmware task
6. Test - Lenovo Notebook - ME/AMT task
7. Test - Lenovo Notebook Software Applications - Lenovo task
Future – Creating a Case

Summary*

CVSS

Priority  Medium

Attributes

glibc  bios  ME  Linux_kernel

BMC  fingerprint  Phoenix  openssl

Intel graphics  AMI  System Update  Nvidia graphics

audio
Solution

1. **Product Attribute Database**
   - Inventory of all supported products and their attributes
   - Links products to supported components and open source/third party code to components

2. **Improved Jira Workflows**
   - SLAs built in

3. **Automated Product tables for Security Advisories**
   - Filters generate product tables for advisories

4. **‘Button Push’ SLA Metrics and Notifications**
   - Improved SLA reporting capabilities
thanks.
Different is better