Handling vulnerabilities in the value chain

MARTIN HÖST, LTH

Research projects (Vinnova funded)

Seconds

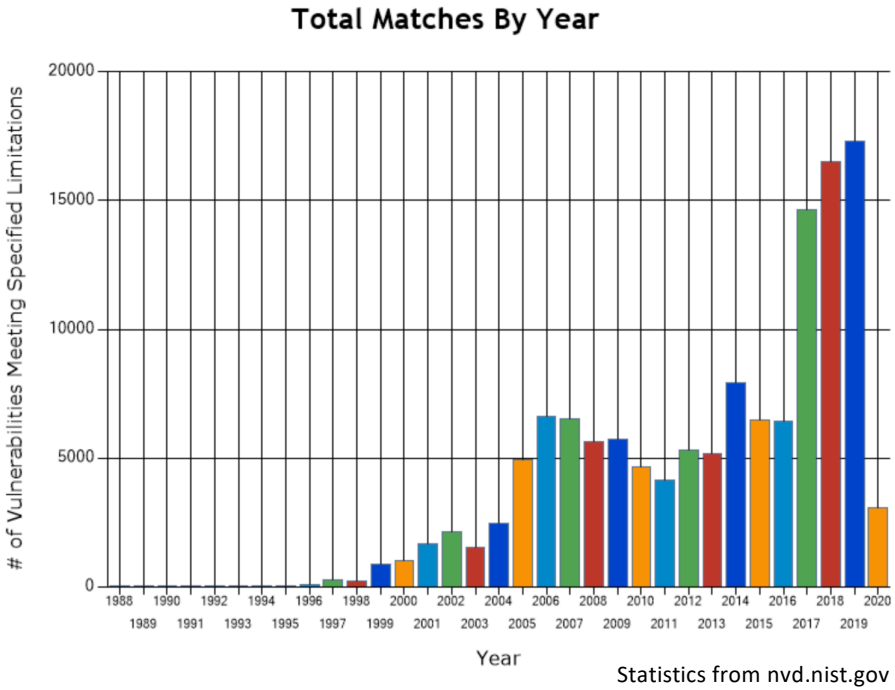
- 2 univ. partners, 7 industry partners
- Problem understanding
- Tool support for product developers
- Process guidelines

HATCH

- 2 univ. partners, 3 industry partners
- Focus on product development and system integration
- Support for product integrators
- Evaluations of tool support and process guidelines

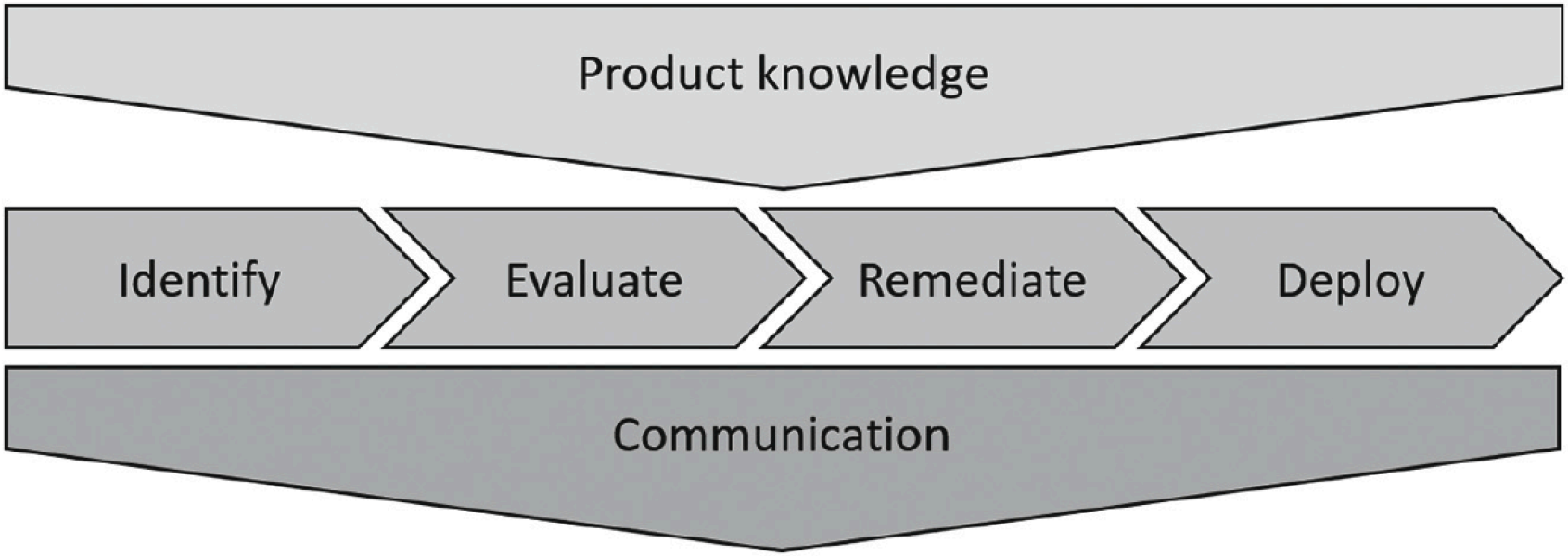
Vulnerabilities in software systems

- Open source is used in (for example) IoT systems to obtain high quality and at the same time be competitive
- Information about vulnerabilities available (and exploits)
- Importance of understanding vulnerabilities increases
  - Attacks can have serious consequences



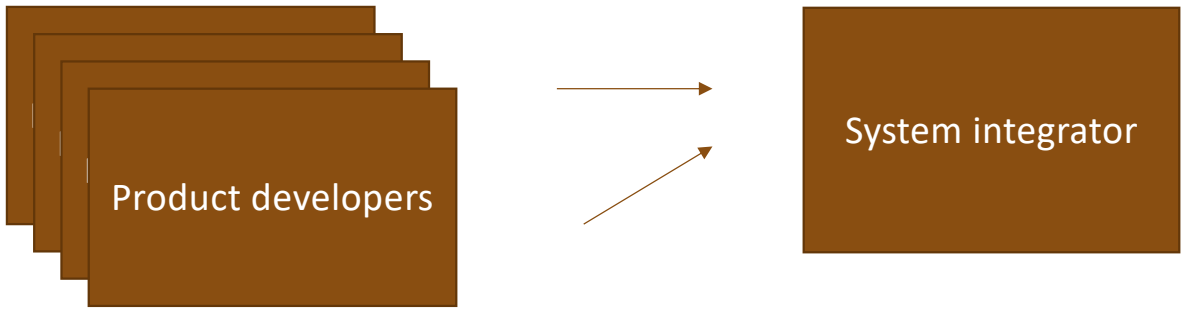
Statistics from nvd.nist.gov
Mar 2, 2020

Approaches for managing vulnerabilities (product developer)



[Pegah Nikbakht Bideh, Martin Höst, Martin Hell, "HAVOSS: A Maturity Model for Handling Vulnerabilities in Third Party OSS Components", in proceedings of International Conference of Product Focused Software Development and Process Improvement (PROFES), 2018]

Building systems with products

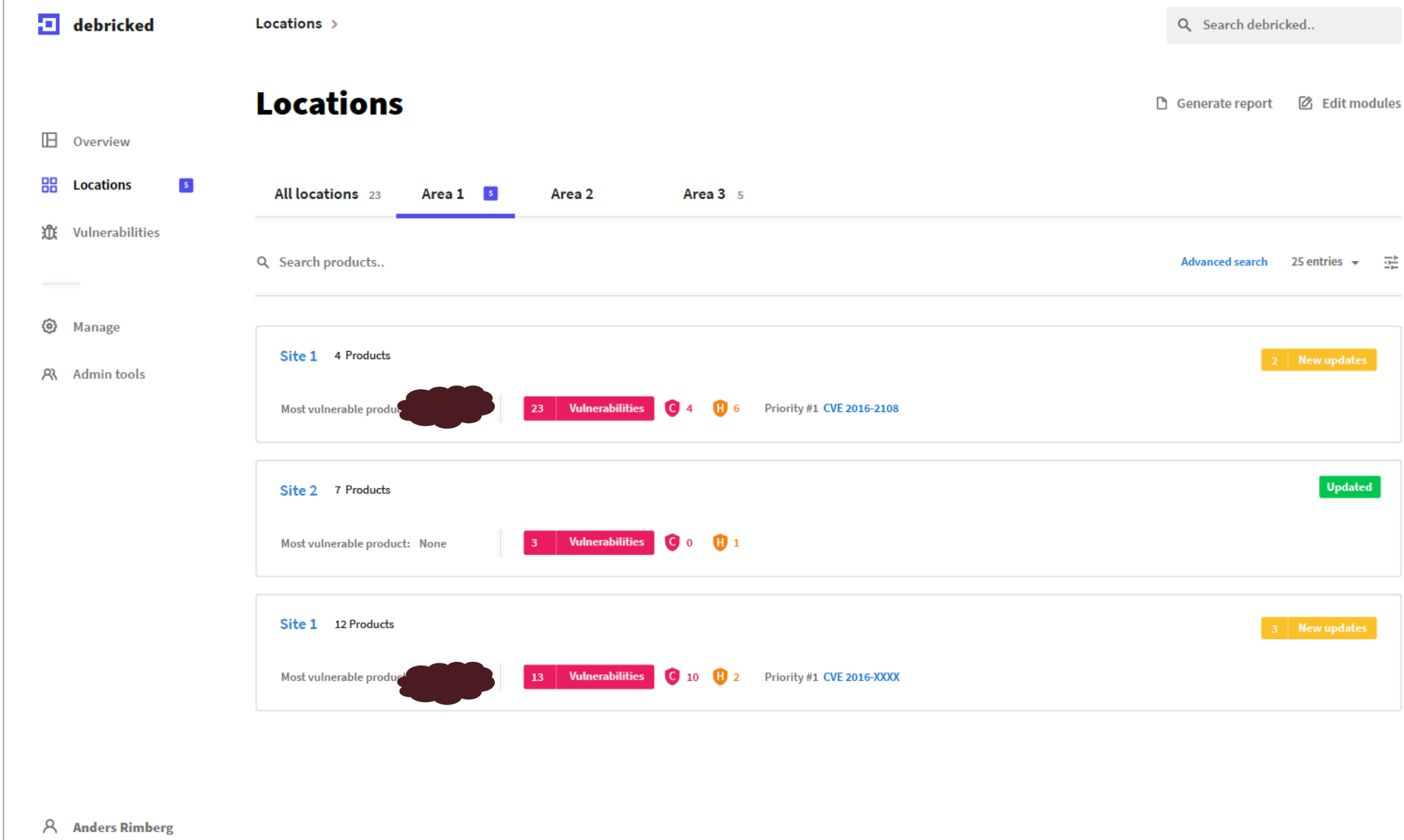


* Want to know about vulnerabilities
* Analyze different versions/products
* Detailed access to product sw

* Wants to know about vulnerabilities
* Analyzes different systems
* Less detailed access to product sw
* Possibility to communicate with developers (and customers)
* Wants information on “rather high level”

Research activities

- Literature surveys
- Interview studies
- Case studies
- Demonstartor building & evaluation


debricked
Locations
Search debricked..
Locations
Generate report
Edit modules
Overview
Locations 5
Vulnerabilities
Manage
Admin tools
All locations 23
Area 1 5
Area 2
Area 3 5
Search products..
Advanced search
25 entries
Site 1 4 Products
2 New updates
Most vulnerable produ
23 Vulnerabilities
C 4
H 6
Priority #1 CVE 2016-2108
Site 2 7 Products
Updated
Most vulnerable product: None
3 Vulnerabilities
C 0
H 1
Site 1 12 Products
3 New updates
Most vulnerable produ
13 Vulnerabilities
C 10
H 2
Priority #1 CVE 2016-XXXX
Anders Rimberg