Vulnerability Coordination and Disclosure in Japan

Task Force on
Vulnerability Disclosure in Europe
11/29/2017

Takayuki (Taki) Uchiyama
JPCERT Coordination Center
Vulnerability Coordination Group /
Global Coordination Division

Introduction

- Working at JPCERT/CC since 2007
  - —Coordinator of software vulnerabilities with vendors
  - —Trainer for CSIRT capacity building (mostly in AP region)
  - —Involved in various global communities (FIRST, APCERT, CVE, etc.)
  - —Current member of CVE Board

- In a past life,
  - —Consultant to Japanese companies seeking FIPS 140-2 validations
  - —Retirement Plan Consultant

About JPCERT/CC

- Foundation
  - —October, 1996
- Organization status
  - —An independent, non-profit organization
  - —Assigned by Ministry of Economy, Trade and Industry (METI) to coordinate vulnerabilities with vendors
  - —CSIRT with national responsibility
- Constituency
  - —Internet users in Japan, mainly for enterprises

About JPCERT/CC

Prevent
Vulnerability Coordination

Watch
- Information analysis
- Internet Traffic Monitoring

Respond
Incident Handling

Early Warning Information Service

Artifact Analysis

Industrial Control System Security

Capacity Building for CSIRTs

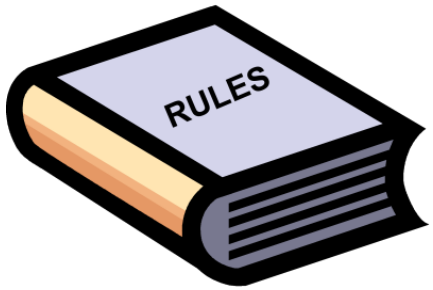
Local Community Development

International Collaboration

VULNERABILITY COORDINATION FRAMEWORK

Way back when…

- July 2004: Ministry of Economy, Trade and Industry (METI) issued notification No. 235 - “Standards for Handling Software Vulnerability Information and Others”
  - The ‘rulebook’ for vendor coordination - “Information Security Early Warning Partnership”
  - This partnership was created in cooperation with several industry organizations
  - JPCERT/CC coordinates with product vendors
  - The scope for the rest of the talk will be software / product vulnerability coordination and disclosure

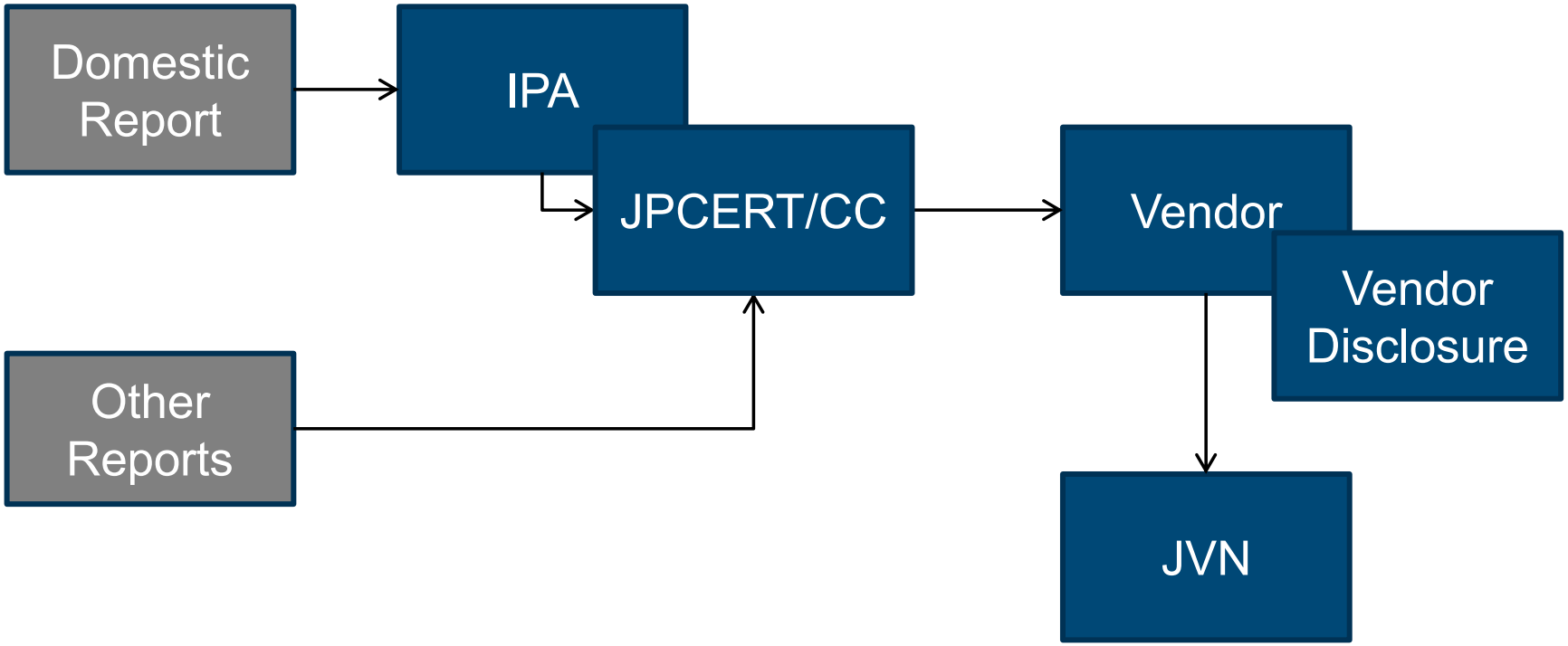


What was expected to be achieved?

- Coordination between researchers and vendors through 3rd party organization
  - —to avoid anonymous full-disclosure
  - —researcher can tell someone responsible about what they found
  - —increase vendor ‘acceptance’ of vulnerability reports

- “Standardization” of (expected) vendor’s response to vulnerability
  - —handling
  - —disclosure
  - —(this was in a world prior to ISO 29147 / ISO 30111)

Basic Flow of the Handling Framework



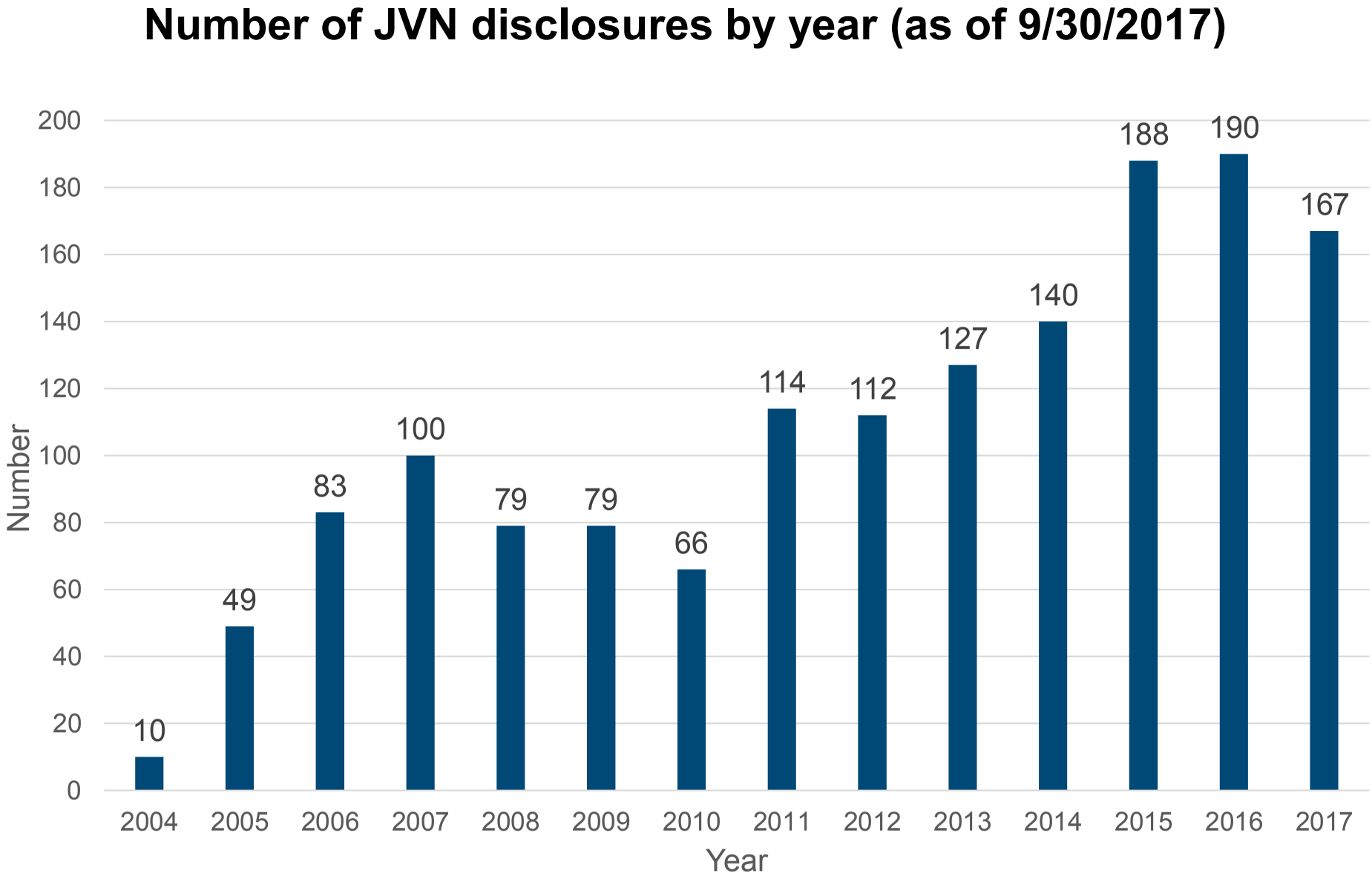
Coordinating the ‘Japanese’ way

- ALL vulnerabilities reported must be coordinated with a vendor until a vendor fix is provided and an advisory on Japan Vulnerability Notes (JVN) is published

- Prioritization is minimal
  - —All cases go through the same processes
  - —Lots of cases remain ‘unresolved’
    - May be fixed (or not)
    - No response
    - Have no idea

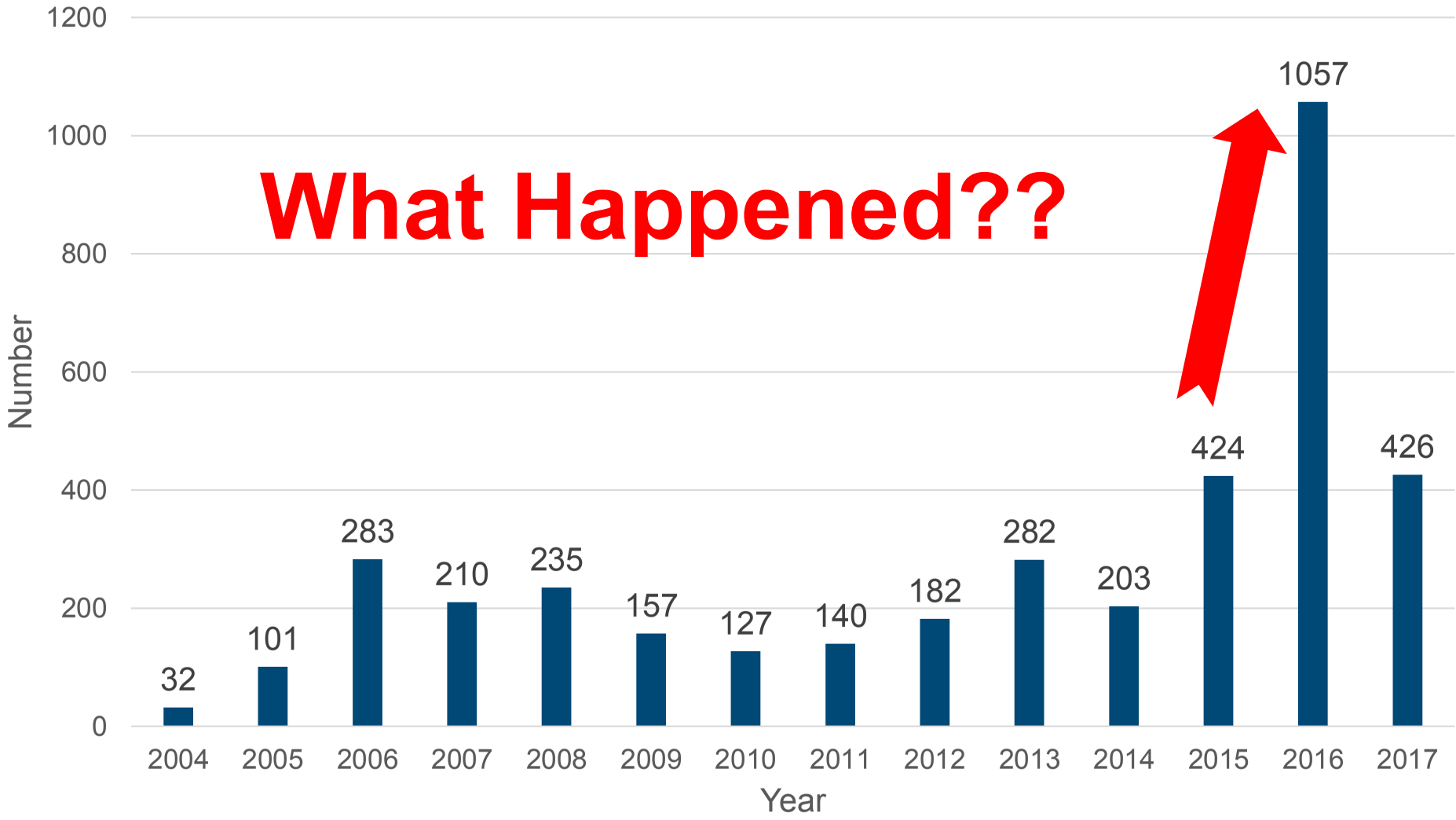
- Within Japanese framework, a case is not “officially closed” unless disclosed on JVN

Since 2004…



Since 2004…

Total number of reported vulnerabilities by year (as of 9/30/2017)



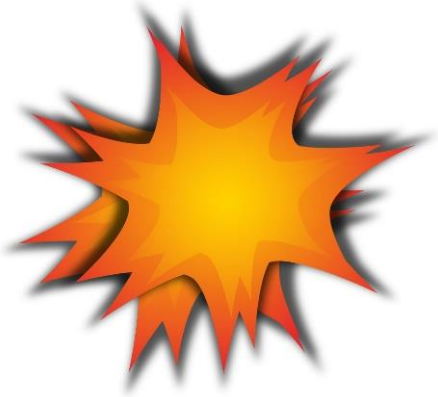
2016 in Review

- Massive increase in number of reports
  - —From a small set of researchers
  - —Large Batches of reports on specific product / vuln types:
    DLL pre-loading in various installers
    Mainly XSS, SQLi in various CMS software
    Mainly XSS, SQLi in WordPress plugins
  - —Unclear of the purpose of this research…

- Increase in internal resources have allowed us to increase output
- But, Input >>>>>>>>> Output

Process Overflow

- Limit to what we can process
  - —Taken to the limit and beyond in 2016



- Lots of ‘fringe’ and low-quality reports
  - —Takes a lot of time to go through
  - —Want vendors to spend as little time possible ‘understanding’ report and more time on addressing issue
  - —Difficult balancing act
- Desperate need to simplify / automate some processes
  - —Vuln reports are not getting to vendors timely right now
  - —JVN disclosure notwithstanding, want to get reports to vendors so that the vulns can get addressed

Process Overflow

- Setup of handling / coordination processes did not consider mass reporting
  - —Became issue in 2016, but was always an underlying issue

Considerations for a Coordination Framework

- Provide an incentives to reporters
  - No monetary incentives
  - Credit is provided upon JVN disclosure
  - Looks good on resume / organizational evaluations
- Provide an incentive to vendors
  - The reason why it's a "Notification" and not a "Law / Policy" is to promote that vendors take their own actions to address vulnerabilities
  - Addressing and disclosing vulnerabilities shows that a vendor's "Security Posture" is good
- Where do 3rd party coordinators fit?
  - Disclose issues so that it reaches a wide audience
  - Support in coordination where multiple parties need to be contacted at the same time

Considerations for a Coordination Framework

- Current Issues
  - —How to handle vulnerabilities that do not have a “wide-effect” to our constituents?
  - —Lots of vulnerability reports that have a low impact
  - —# of Reports >>>>> What are resources can handle
  - —In Japan, there are very few vendors / developers that can handle vulnerabilities reported directly by researchers
    - Lack of triage ‘standard’
    - Do not know how to communicate with researcher
    - Overall lack of know-how in handling vulnerabilities
    - ISO 29147 / ISO 30111 has helped in this regard but still a long way to go

Thank you!

For inquiries on JVN:
jvn@jvn.jp
For vulnerability reports
vuls@jpcert.or.jp
For any other vulnerability related inquires
vultures@jpcert.or.jp