RSA CONFERENCE 2013

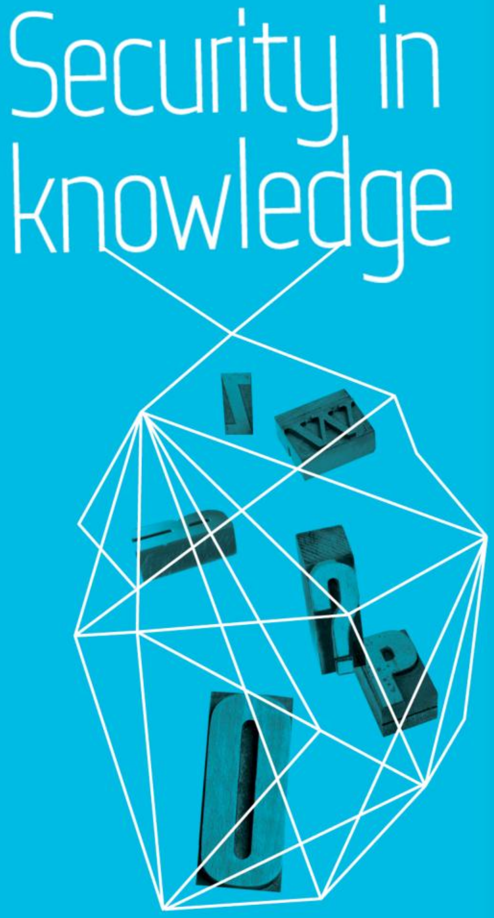
APPLICATION SECURITY RESPONSE: WHEN HACKERS COME A-KNOCKING

Katie Moussouris

Senior Security Strategist

Microsoft Security Response Center

http://twitter.com/**k8em0** (that's a zero)



Session ID: ASEC-T18

Session Classification: Intermediate

Agenda

- Introductions
- A Tale of Two Standards – ISO 29147 and 30111
- ISO 29147 Vulnerability Disclosure Overview
- ISO 30111 Vulnerability Handling Processes Overview
- Technical Capabilities for Handling Vulnerabilities
- Communication Capabilities – Say what?!
- Other Considerations -
- Timing for Publication
- Taking it all In – And Applying It to Scale
- Questions for the Editor

RSACONFERENCE2013

A Tale of Two Standards – for the best and worst of times

Who Am I

- Joined Microsoft in April 2007
- Now I run Microsoft Security Community Outreach & Strategy, MSVR, and BlueHat ☺
- My (Security*) Work in Bullet Points:
  - Linux Dev and Security Tzarina - TurboLinux, circa 2000
  - Pen Tester - Artist formerly known as @stake
  - Founder - Symantec Vulnerability Research (SVR)
  - Founder - Microsoft Vulnerability Research (MSVR)
  - Policy Maker
    - Editor for draft ISO standard on Vulnerability Handling (30111)
    - Lead SME for US National Body on Vulnerability Disclosure (29147)

* Was a molecular biologist in a past professional life, worked on the Human Genome Project

A Tale of Two Standards

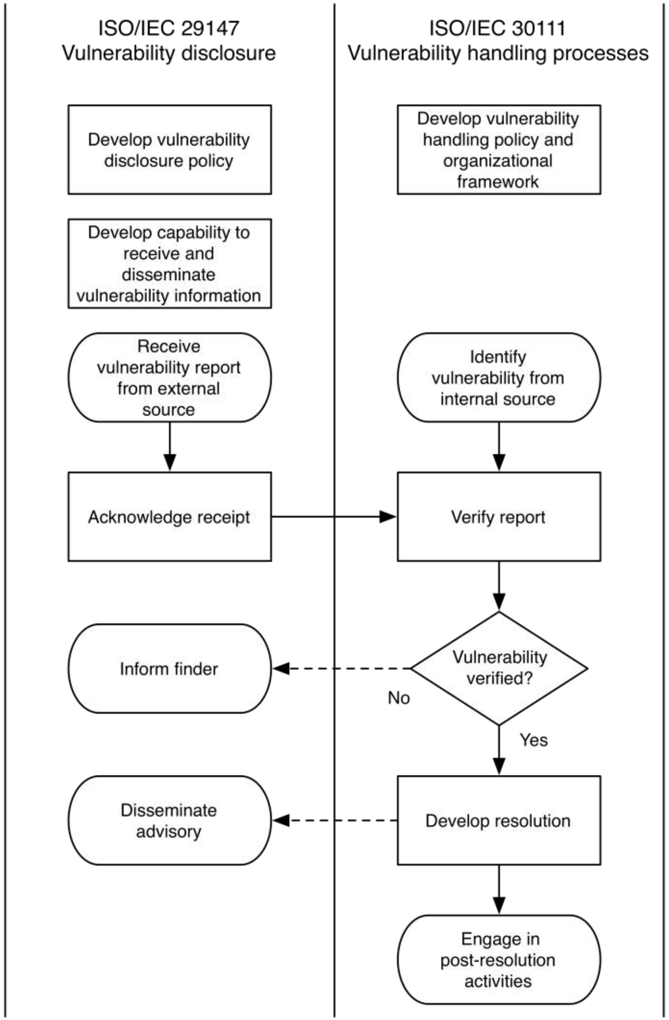
ISO Standard on Vulnerability Disclosure (29147)

- How vendors should deal with vulnerability reports from “external finders” (AKA: Hackers)

ISO Standard on Vulnerability Handling Processes (30111)

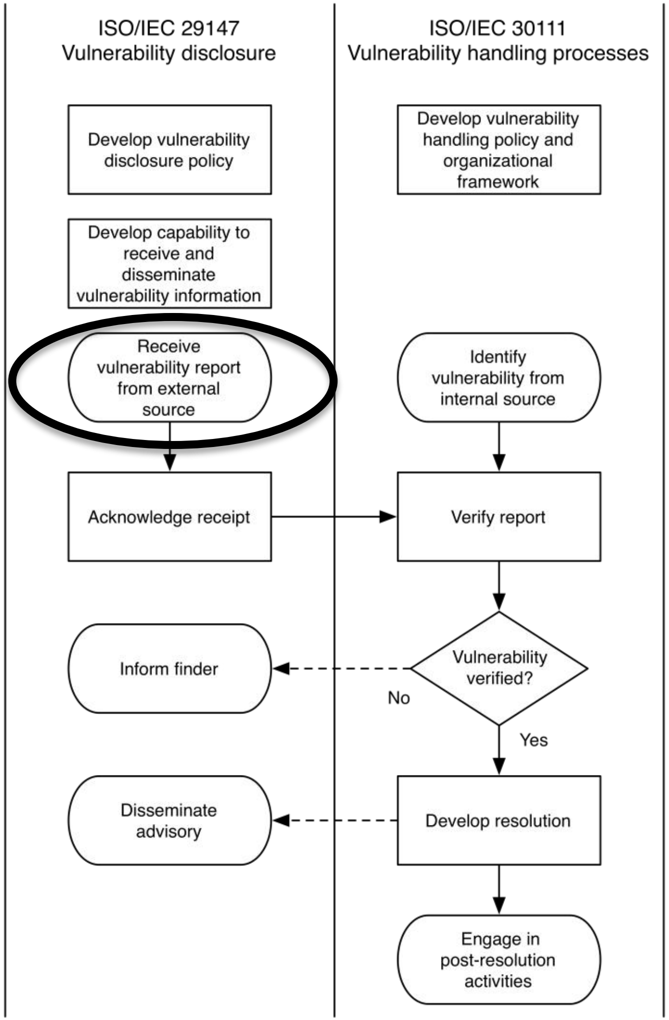
- How vendors should investigate, triage, and resolve ALL potential vulnerabilities, whether reported from external finders, or via the vendor’s internal testing

Interconnection: 29147 and 30111


ISO/IEC 29147
Vulnerability disclosure
ISO/IEC 30111
Vulnerability handling processes
Develop vulnerability disclosure policy
Develop vulnerability handling policy and organizational framework
Develop capability to receive and disseminate vulnerability information
Receive vulnerability report from external source
Identify vulnerability from internal source
Acknowledge receipt
Verify report
Inform finder
Vulnerability verified?
No
Yes
Disseminate advisory
Develop resolution
Engage in post-resolution activities

Interconnection: 29147 and 30111

KNOCK KNOCK!



ISO/IEC 29147
Vulnerability disclosure

ISO/IEC 30111
Vulnerability handling processes

Develop vulnerability disclosure policy

Develop vulnerability handling policy and organizational framework

Develop capability to receive and disseminate vulnerability information

Receive vulnerability report from external source

Identify vulnerability from internal source

Acknowledge receipt

Verify report

Vulnerability verified?

No

Yes

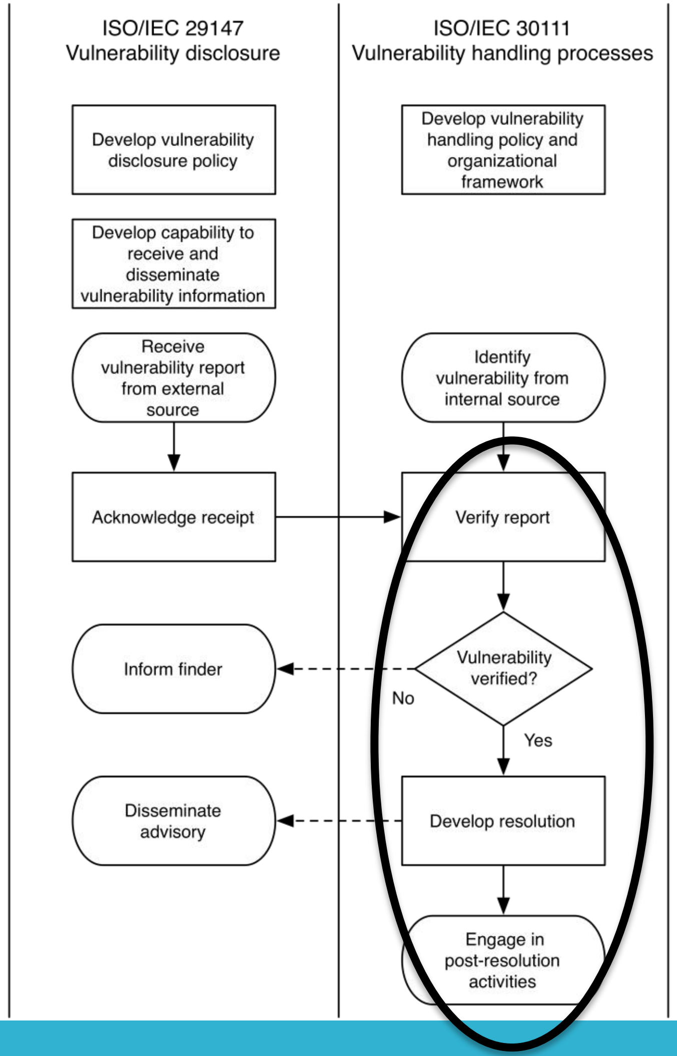
Inform finder

Disseminate advisory

Develop resolution

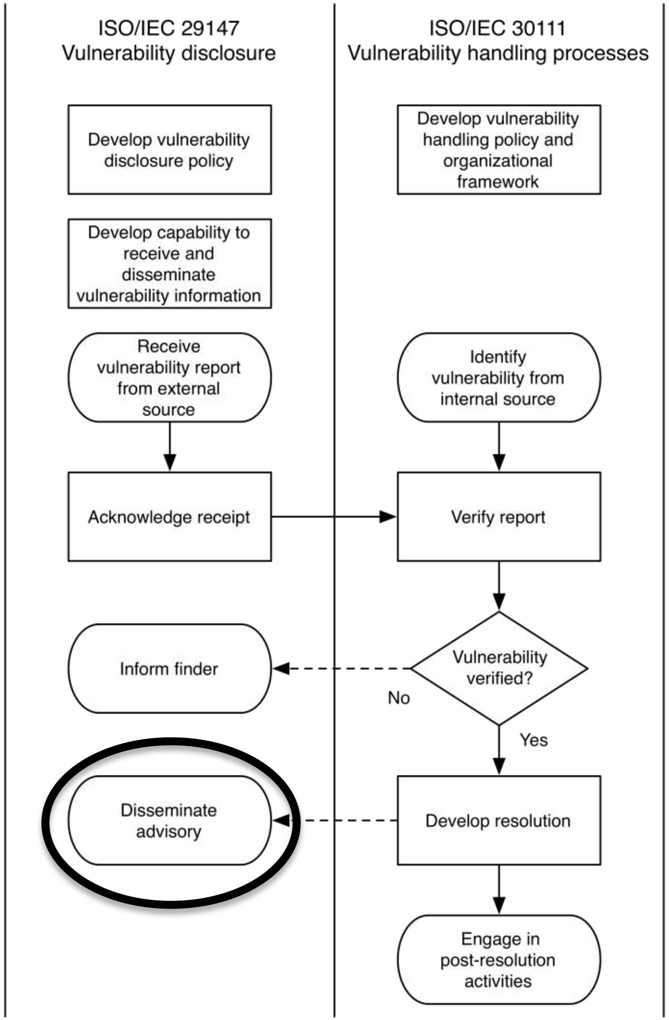
Engage in post-resolution activities

Interconnection: 29147 and 30111


ISO/IEC 29147
Vulnerability disclosure
ISO/IEC 30111
Vulnerability handling processes
Develop vulnerability disclosure policy
Develop vulnerability handling policy and organizational framework
Develop capability to receive and disseminate vulnerability information
Receive vulnerability report from external source
Identify vulnerability from internal source
Acknowledge receipt
Verify report
Inform finder
Vulnerability verified?
No
Yes
Disseminate advisory
Develop resolution
Engage in post-resolution activities

DON'T PANIC!

Interconnection: 29147 and 30111

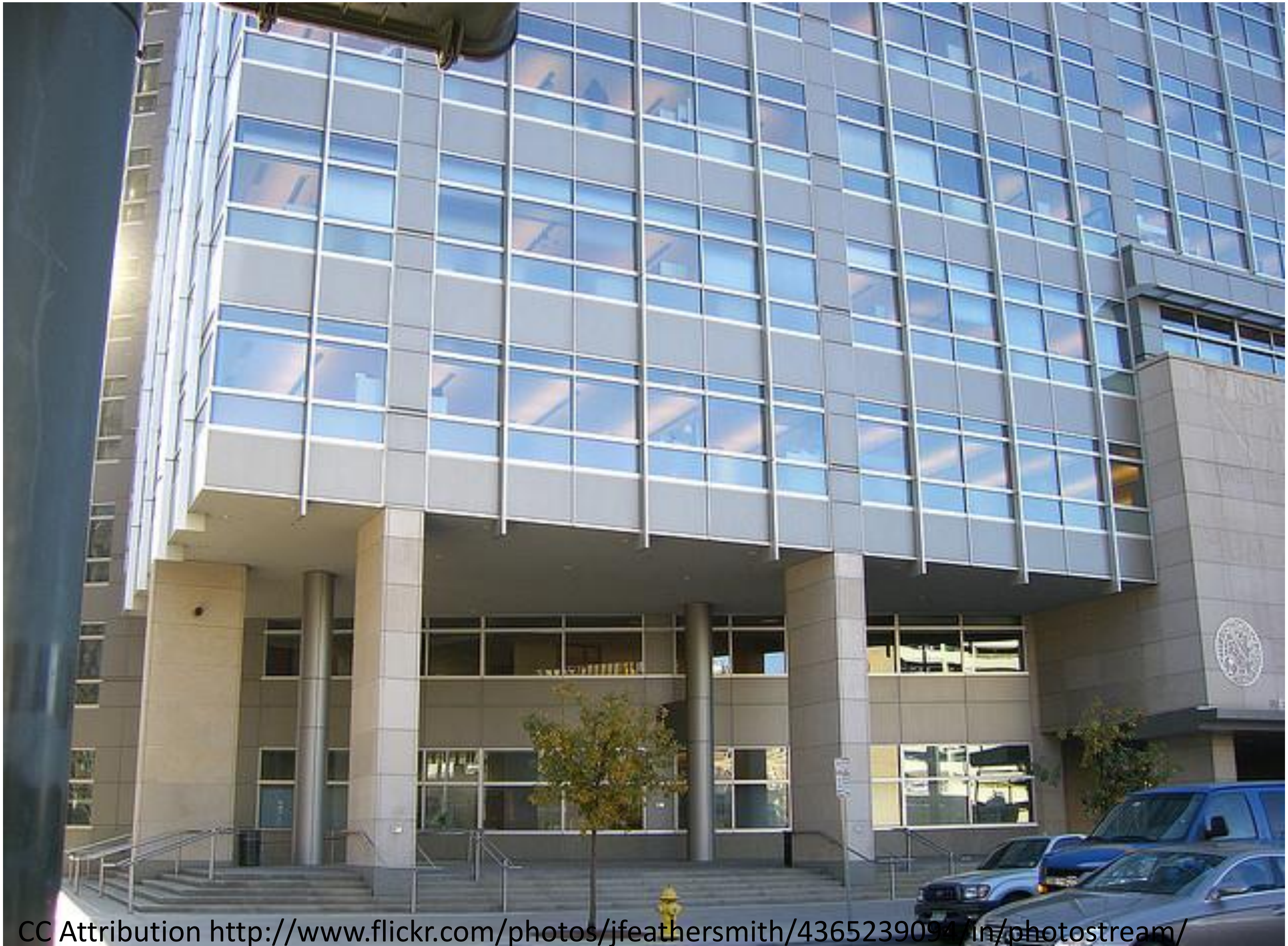

ISO/IEC 29147
Vulnerability disclosure
ISO/IEC 30111
Vulnerability handling processes
Develop vulnerability disclosure policy
Develop vulnerability handling policy and organizational framework
Develop capability to receive and disseminate vulnerability information
Receive vulnerability report from external source
Identify vulnerability from internal source
Acknowledge receipt
Verify report
Inform finder
Vulnerability verified?
No
Yes
Disseminate advisory
Develop resolution
Engage in post-resolution activities

ALL BETTER!

RSA CONFERENCE 2013

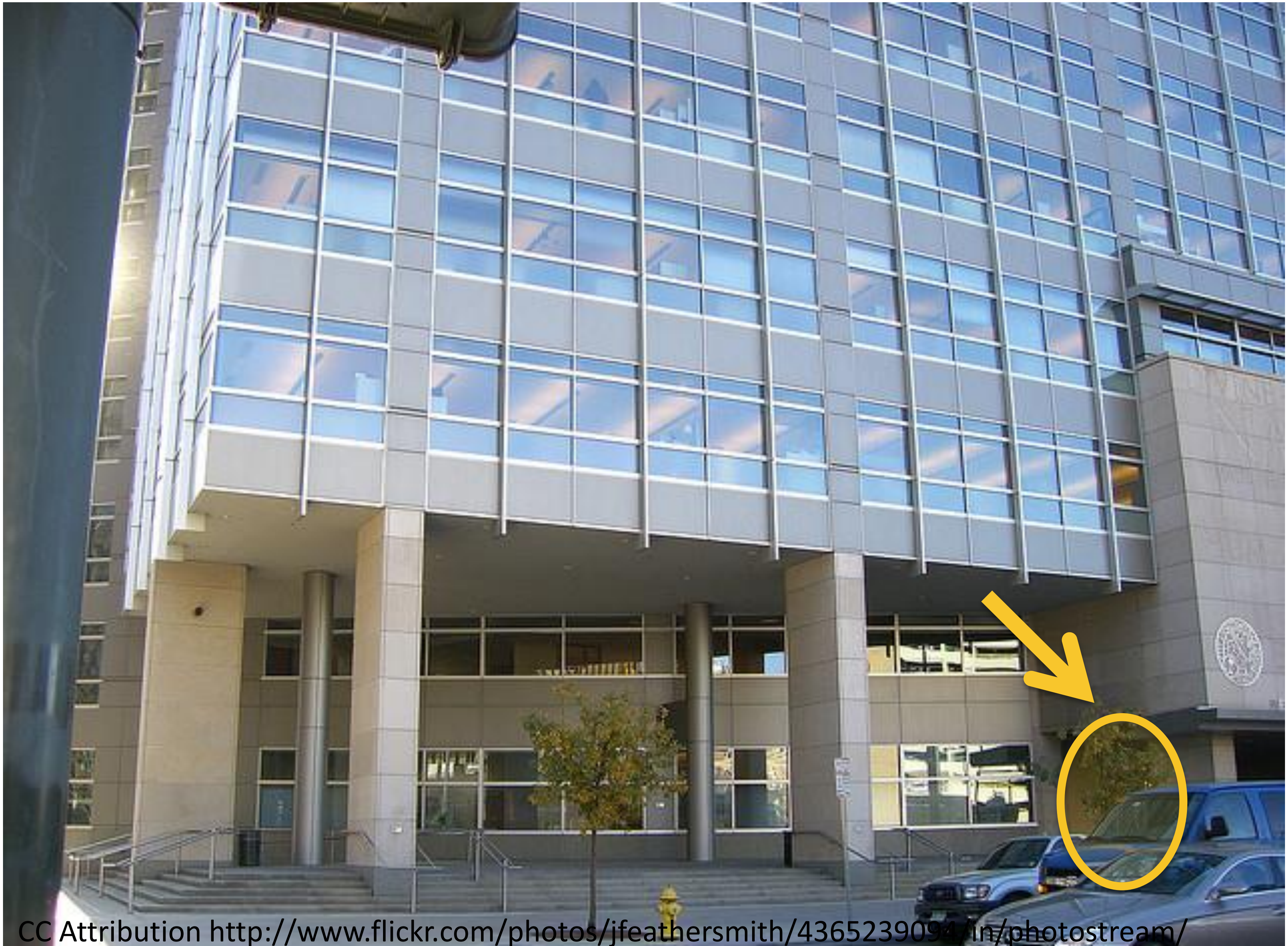
Receiving Vuln Reports – The Easy Way

Where is the Front Door?



CC Attribution http://www.flickr.com/photos/jfeathersmith/4365239094/in/photostream/

Where is the Front Door?



CC Attribution http://www.flickr.com/photos/jfeathersmith/4365239094/in/photostream/

Where There's A Will…

CC Attribution http://www.flickr.com/photos/grizdave/1327304418/in/photostream/

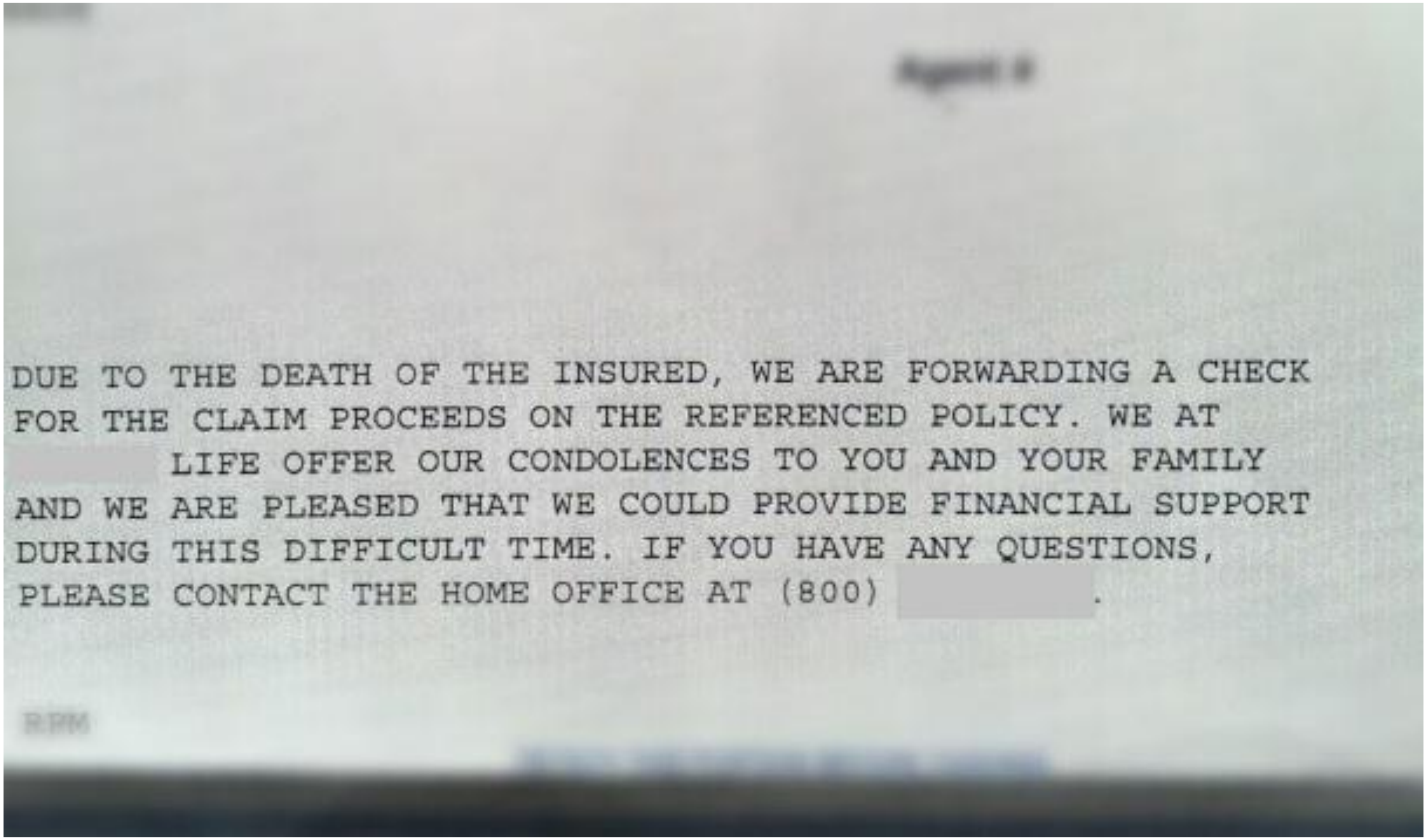
Red Carpet or Welcome Matt

CC Attribution http://www.flickr.com/photos/theotherdan/517315445/

Got it! Now what?

Acknowledge Receipt of the Report

Autoreply Good Enough?



DUE TO THE DEATH OF THE INSURED, WE ARE FORWARDING A CHECK FOR THE CLAIM PROCEEDS ON THE REFERENCED POLICY. WE AT [redacted] LIFE OFFER OUR CONDOLENCES TO YOU AND YOUR FAMILY AND WE ARE PLEASED THAT WE COULD PROVIDE FINANCIAL SUPPORT DURING THIS DIFFICULT TIME. IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT THE HOME OFFICE AT (800) [redacted].

CC Attribution http://www.flickr.com/photos/_ellie_/8252498753/in/photostream/

Vendors: Ask for This Information

- Affected Product(s)/versions/URLs
- System Details (Operating System, etc.)
- Technical Description and Repro Steps
- PoC
- Other Parties/Products Involved
- Disclosure Plans/Dates

Dear Vuln Abbey: What Should the Advisory Say in Polite Company?

Example Advisory Excerpt

- Active Directory Invalid Free Vulnerability - CVE-2009-1138
- A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
- View the full advisory at http://www.microsoft.com/technet/security/bulletin/ms09-018.mspx

Example Advisory Excerpt

- Active Directory Invalid Free Vulnerability - CVE-2009-1138
- A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
- View the full advisory at http://www.microsoft.com/technet/security/bulletin/ms09-018.mspx

Example Advisory Excerpt

- Active Directory Invalid Free Vulnerability - CVE-2009-1138
- A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
- View the full advisory at http://www.microsoft.com/technet/security/bulletin/ms09-018.mspx

Example Advisory Excerpt

- Active Directory Invalid Free Vulnerability - CVE-2009-1138
- A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
- View the full advisory at http://www.microsoft.com/technet/security/bulletin/ms09-018.mspx

Example Advisory Excerpt

- Active Directory Invalid Free Vulnerability - CVE-2009-1138
- A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
- View the full advisory at http://www.microsoft.com/technet/security/bulletin/ms09-018.mspx

Vulnerability Disclosure Standard (29147)

- Vendors should have a clear way to **receive** vuln reports
- Vendors should **acknowledge receipt** of vuln reports within **7 calendar days**
- Vendors should **coordinate** with finders
- Vendors should issue **advisories** that contain useful information, at a minimum:
  - Some Unique Identifier
  - Affected products
  - Impact/severity of damage if vuln is exploited
  - How to eliminate or mitigate the issue (guidance or patching instructions)
- **Generally a good idea** to give **finders credit in the advisory** if the finder wishes to be publicly acknowledged.

Great…But You Skipped the Good/Hard Parts! How to Investigate and Remediate?!

Remember: Don’t Panic !

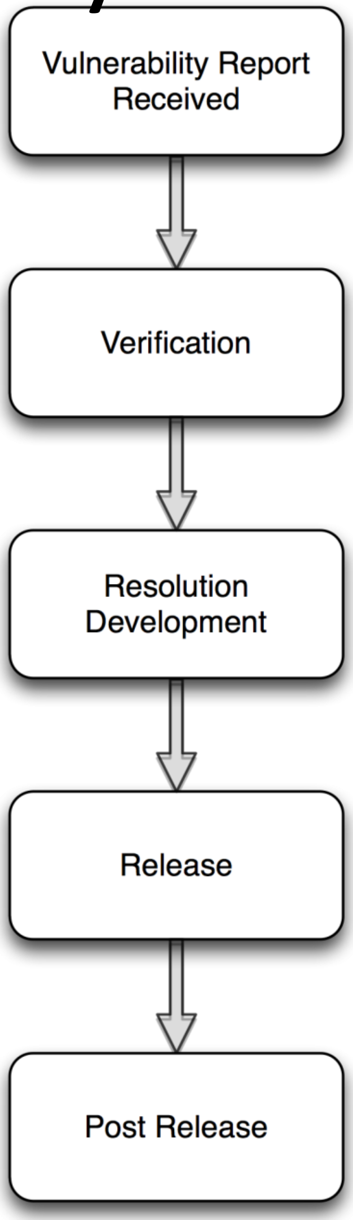
Vulnerability Handling Standard (30111)

- Vendors should have a **process** and **organizational structure** to support vuln investigation and remediation
- Vendors should perform **root cause analysis**
- Vendors should weigh various **remediation** options to adjust for real world risk factors
  - Balance speed with thoroughness
- Vendors should try to **coordinate** with other vendors if appropriate
  - multi-vendor issues
  - supply chain issues

Vulnerability Response Capability Areas

- **Policy**
  - Why Response?
- **Organizational Capabilities**
  - Who’s in charge of Response?
- **Engineering Capabilities**
  - How quickly, effectively, and thoroughly do we respond?
- **Communication Capabilities**
  - How clear and timely is our guidance?
- **Analysis Capabilities**
  - How can we learn from this to prevent more vulns? Can we predict trends to aid in investment of resources?

Vulnerability Handling Process



Vulnerability Report Received

Verification

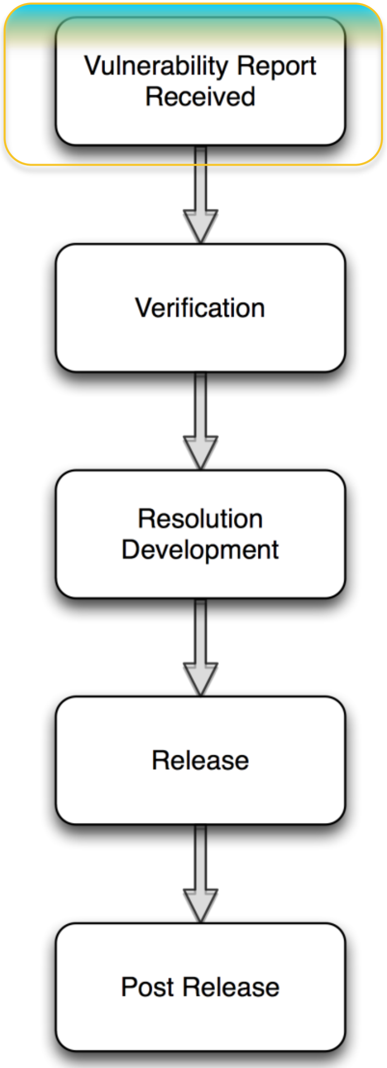
Resolution Development

Release

Post Release

Vulnerability Report Received

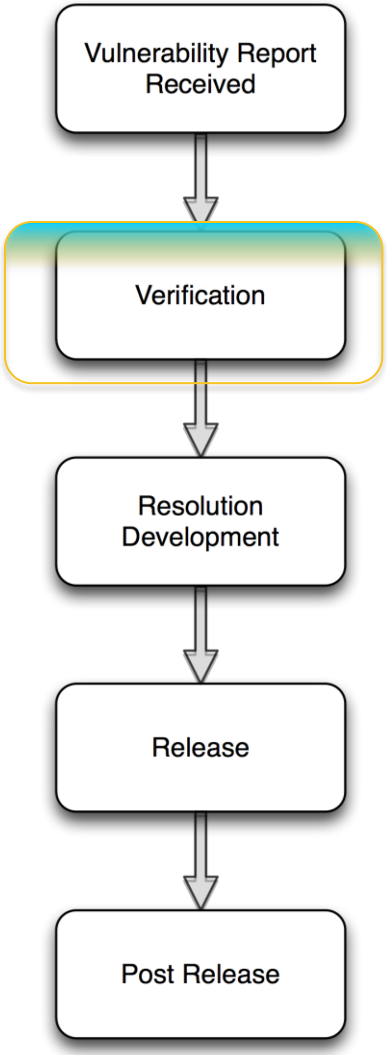
- External finder vs Internal testing
  - Overall process is similar, but risks may change
- If an external finder was involved, follow 29147 to
  - Understand the communication expectations
  - Take into consideration the finder’s intentions and publication plans during the resolution development phase



Verification – Steps*

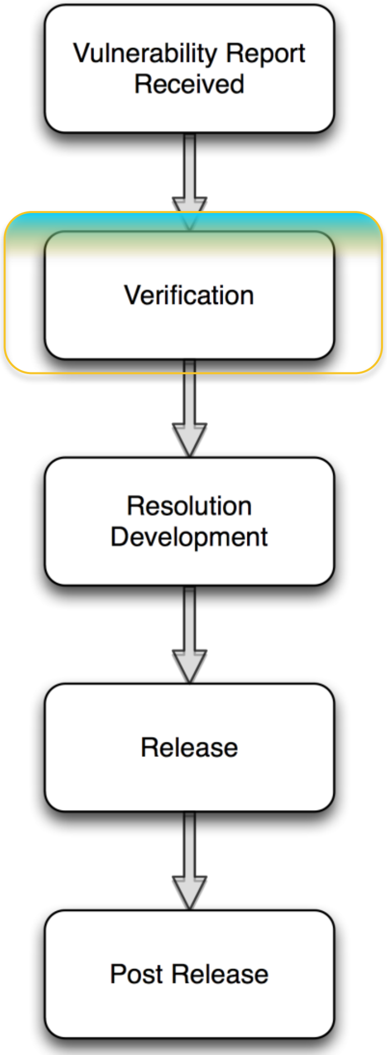
- **Initial Investigation**: The vendor attempts to confirm the potential vulnerability
- **Root Cause Analysis**: The vendor attempts to determine the underlying cause of the vulnerability
- **Further Investigation**: The vendor attempts to find other instances of the same type of vulnerability in the product or service, or in other products.
- **Prioritization**: The vendor considers the threat posed by the vulnerability to affected users of the product or online service.
  - For each affected product or online service, there may be different severities of the same underlying issue.

* Some processes may occur in parallel, rather than sequentially



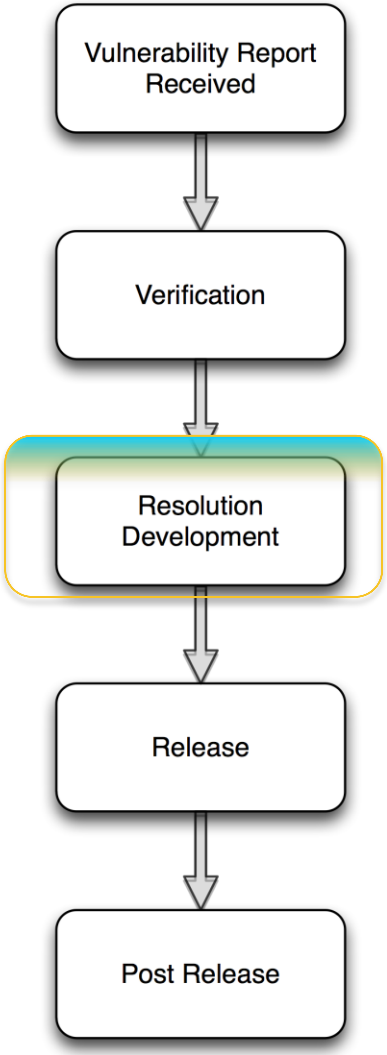
Verification – Possible Exit Conditions

- **No Repro**: The bug could not be reproduced.
  - If reported by an external finder, see 29147 before closing the case
- **Duplicate Bug**: The issue is a duplicate vulnerability and is already being addressed via this process or is already fixed.
- **Obsolete Product Bug**: The vulnerability is in a product that is no longer supported by the vendor.
- **Non-security Bug**: The issue is a bug that either has no security implications, or is not exploitable with currently known techniques.
  - Vendors need to keep up with current exploitation techniques
- **Third-party Bug**: The vulnerability is due to third-party code, configurations, or is present in a specification for which the vendor is not directly responsible.



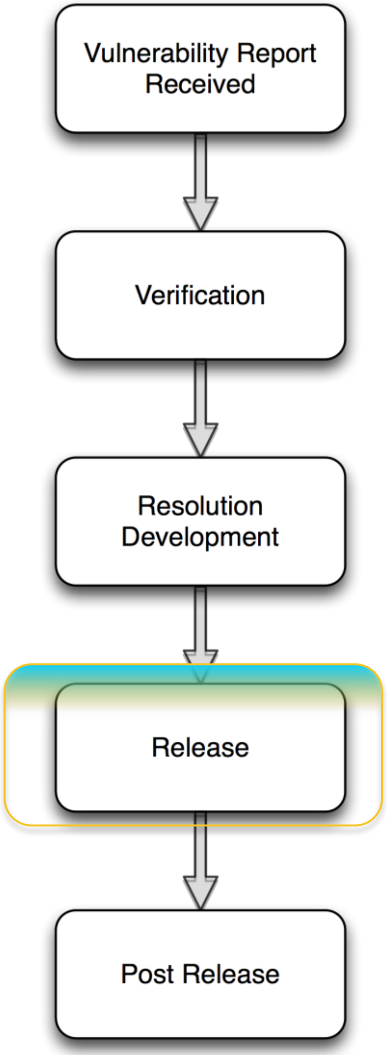
Resolution Development

- **Resolution decision**: The vendor determines how the vulnerability can be resolved comprehensively, how to reduce the impact of successful exploitation of the vulnerability, or how to reduce exposure.
- **Produce Remediation**: The vendor produces patch(es), fix(es), upgrade(s), or documentation or configuration change(s) to address a vulnerability.
- **Test Remediation**: The vendor develops and performs appropriate tests to ensure the vulnerability issue has been addressed on all supported platforms.



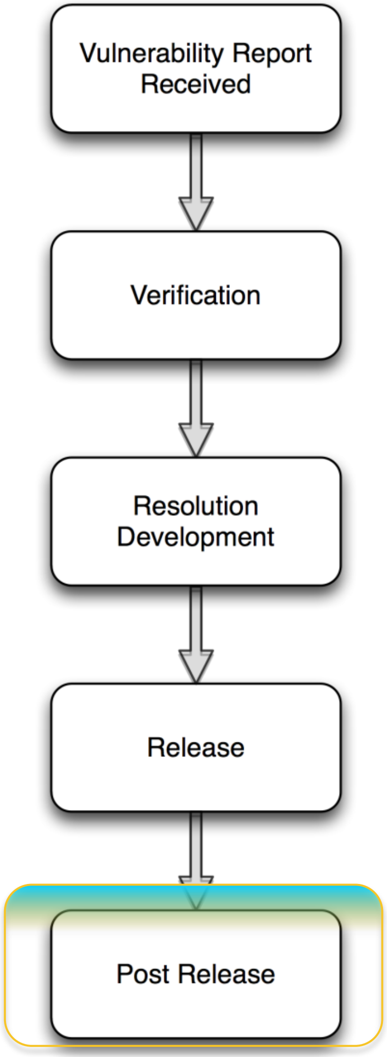
Release

- **Online service vulnerability resolution**: Follow your organizations‘ update deployment or configuration change processes for production systems.
- **Product vulnerability resolution**:
- For vulnerabilities in products where affected users must take some action to protect themselves (e.g. Install a patch)
- Release the remediation via an advisory, as outlined via the processes defined in ISO/IEC 29147.



Post Release

- **Case maintenance**: After the resolution has been released, further updates to the resolution might continue.
- **Security development lifecycle feedback**: The vendor updates the development lifecycle using information gained during root cause analysis to prevent similar vulnerabilities in new or updated products or services. (see 27034)
- **Monitoring**:
  - For online services vulnerabilities, after the vendor applies the remediation, the vendor should monitor the stability of the product or service.
  - Post-patch release monitoring for exploitation can help focus communication to most affected users.



Communication: Know What to Say and When to Say It

Communication: Say What?!

- Communication with external finders
  - Have a secure method such as PGP to communicate technical details
  - Convey fix timelines and schedule slips
- Communication with product business divisions
  - Have an SLA in place for internal teams for both emergencies and non-emergencies
  - Response Team should update with developments in threat landscape
- Communication with coordinators or other vendors
  - Get to know your counterparts at other vendors
- Communication with affected users
  - Establish a verifiable communication channel to alert users of threats

RSA CONFERENCE 2013

Other Vulnerability Handling Process Considerations

Monitoring Vulnerability Handling Phases

- **Speed**: Vendors should monitor the time it takes to address a vulnerability through this process and try to speed up without losing quality.
- **Completeness**: Vendors should monitor the completeness of the remediation, to ensure that it addresses the root cause of the vulnerability.
- **Persistence**: Vendors should monitor the remediation's effectiveness after it is released to affected users.

Confidentiality of Vulnerability Information

- Vendors should take care to maintain the confidentiality of sensitive vulnerability information.
  - Any **PII** associated with the vulnerability report (e.g. stolen SSNs, or the finder's info, if they wish to remain anonymous)
  - Vulnerability information that is not yet published or widely known, for which there is no defense yet, such as **technical details that inordinately benefit attackers**
- Premature disclosure of sensitive vulnerability information can increase the costs and risks associated with disclosure for vendors and users.
  - Vendors should take reasonable steps to protect vulnerability information, as they would any HBI data.

Supply Chain! Multi-Vendor!

- If the vuln is part of another vendor’s supply chain (either upstream or downstream), or is a multi-vendor issue
  - **Coordinate**: Vendors should attempt to include other affected vendors in the discussion of potential resolutions if possible
- Common Supply Chain/Multi-vendor Scenarios:
  - Vuln affects specific platform(s) due to underlying OS or CPU
  - Flawed standard functional **specification** or in published **algorithms**;
  - vulnerabilities in commonly used **libraries**;
  - vulnerabilities in software components that **lack a current maintainer**.
- This often gets **messy**, so flexibility is key!
  - The focus should be to minimize risk

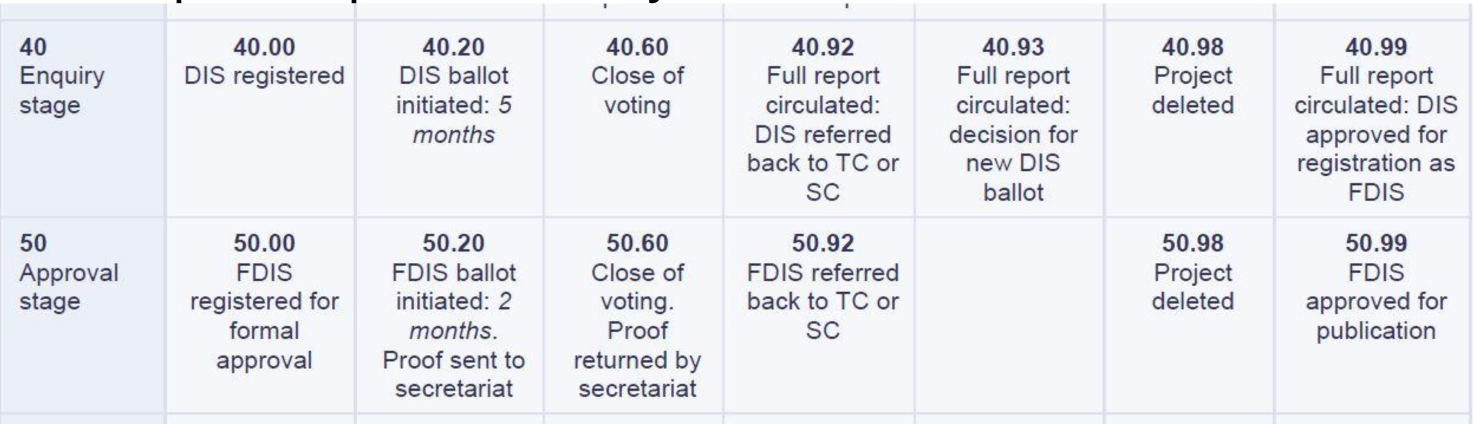
Bonus Pro Tips: For Online Services

- **Not in the Standards, but a Pretty Good Idea**
- Vendors should ask that finders, where possible:
  - Give a reasonable amount of time to fix before going public with technical details of the vuln
  - **Try not to DoS** the online service while looking for vulns
  - **Try not to compromise the PII** of other users
    - E.g. Suggest setting up two test accounts, rather than going after other real users' data
  - **Tell the vendor if PII of other users** was compromised
    - The vendor will likely have to disclose that fact to those users
- Vendors may want to try stating clearly that if the finder follows the above rules, **then the vendor won't take legal action**

Vulnerability Disclosure and Handling Process Standards – Not If But When

Publication Timing

- ISO Standard of Vulnerability Disclosure (29147)
  - The Vote is in! DIS was approved (40.99).
  - Likely publication by end of 2013
- ISO Standard on Vulnerability Handling Processes (30111)
  - DIS registered in October 2012 (40.20)
  - Expected publication by end of 2013



40 Enquiry stage	**40.00** DIS registered	**40.20** DIS ballot initiated: 5 *months*	**40.60** Close of voting	**40.92** Full report circulated: DIS referred back to TC or SC	**40.93** Full report circulated: decision for new DIS ballot	**40.98** Project deleted	**40.99** Full report circulated: DIS approved for registration as FDIS
50 Approval stage	**50.00** FDIS registered for formal approval	**50.20** FDIS ballot initiated: 2 *months*. Proof sent to secretariat	**50.60** Close of voting. Proof returned by secretariat	**50.92** FDIS referred back to TC or SC		**50.98** Project deleted	**50.99** FDIS approved for publication

How ISO Will Affect Vulnerability Handling

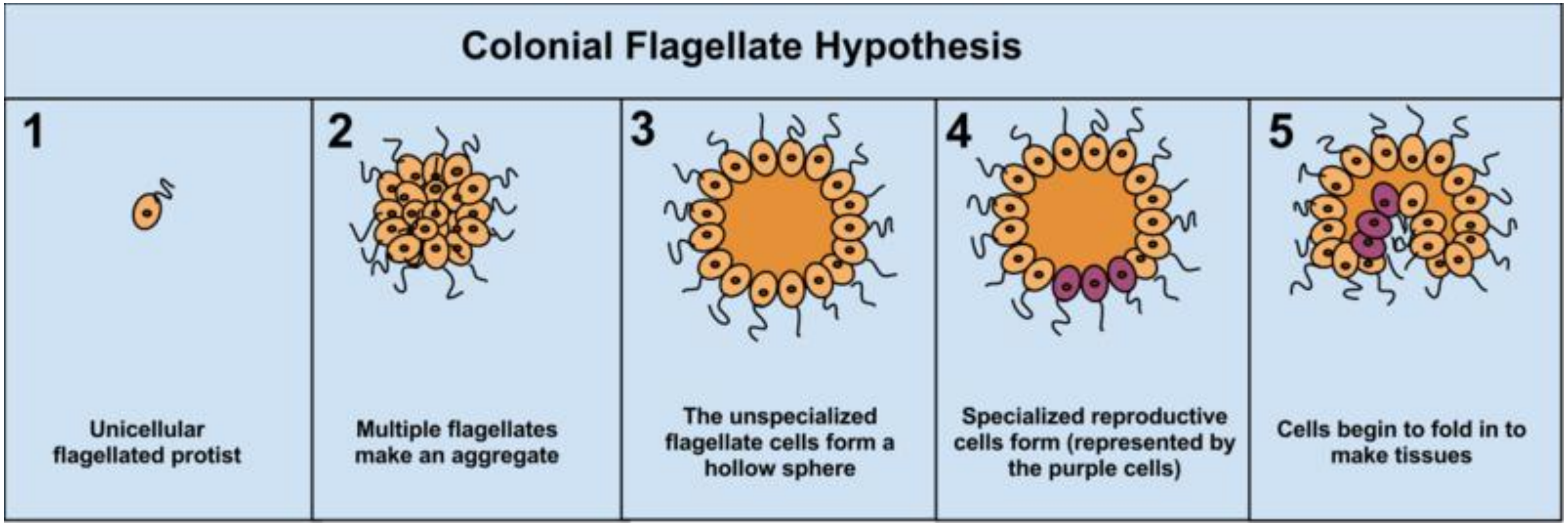
- Vuln Disclosure Standard (**29147**)
  - Help make it **easier for finders to report vulns** to vendors
  - Help make the advisories a vendor releases **more useful**
- Vuln Handling Standard (**30111**)
  - Help raise the level of **security investigation and remediation** that vendors do
  - Help foster appropriate **vulnerability coordination between vendors**

Related Standard – Bringing It Full Circle

- ISO/IEC 27034 Information technology – Security techniques – Application security
  - Root Cause Analysis from 30111 feeds information back into the Security Development Lifecycle
  - Overall improvement of product security depends on learning from one’s mistakes.
- Improving Security Development Saves Orgs Time and Money
  - Can your org afford to keep making the same security mistakes?
  - Investing in Response Helps Stop the Bleeding, but Investing in Secure Development Helps Limit the Wounds

About Scale and Differentiation

- Many Hats: Efficient but Lacks Scalability
- Specialization: Well-resourced but Complex



Colonial Flagellate Hypothesis

1 Unicellular flagellated protist

2 Multiple flagellates make an aggregate

3 The unspecialized flagellate cells form a hollow sphere

4 Specialized reproductive cells form (represented by the purple cells)

5 Cells begin to fold in to make tissues

Vulnerability Handling

- **Policy**
  - Decide to respond, roll out the carpet, and open the front door.
- **Organizational Capabilities**
  - Executive Support, Growth, then Specialization
- **Engineering Capabilities**
  - Got Root (cause)? Balance timing and testing.
- **Communication Capabilities**
  - How do users know they’re vulnerable? How do they fix it?
- **Analysis Capabilities**
  - How can we learn from this and can we predict trends?

CC attribution http://www.flickr.com/photos/m-gem/2268466355/in/photostream/

RSACONFERENCE2013

Questions for the Editor?

http://twitter.com/**k8em0** (that’s a zero)