Can Security Vulnerability Disclosure Processes Be Responsible, Rational *and* Effective?

Toward a Sane Open Source Security Vulnerability Disclosure Process

Larissa Shapiro

December 8, 2011

LISA '11, Boston, MA

http://www.isc.org/

About the Presenter

Larissa Shapiro

ISC Product Manager

larissas@isc.org

@larissashapiro

Agenda

- Vulnerability Disclosure Terminology
  - History and Context
- ISC’s Current Vulnerability Disclosure Policy
  - version 1.1
- New updates for version 1.2
- ISC’s use of Test Driven Development (TDD) and the impact on Vulnerability Disclosure
- Q&A

ISC in a Nutshell

Forum

- BIND
- BIND 10 Working Group
- DHCP
- AFTR / PCP
- SRF
- Open Source Routing

... and more to come.

Professional Services

- Consulting
- Training
- Software Support Services
- Custom Software Development
- F-Root Corporate Node
- DNS SNS-Com
- Full version of Domain Survey

Public Benefit Services

- DNS F-Root
- DNS Secondary Server Resiliency (SNS-PB)
- Hosted@ - hosting a range of open source projects
- Free Domain Survey Report
- Participation in IETF, RIPE WG, ICANN, ARIN, ISOC, UKNOF, etc

Empowerment

- Standards Driver - early implementations of standards based code.
- Policy Meetings - Empowering Spheres of Influence
- Operational Security - Pioneering new approaches to safe guard the Internet (OPSEC-Trust)
- Operational Meetings - (APRICOT, AFNOG, NANOG, LISA, etc)
- Research (DNS OARC)

http://www.isc.org/

Vulnerability Disclosure Terminology

Three Major Vulnerability Management Phases

- There are three main phases to vulnerability management.
  - Phase 1 – Vulnerability Reporting, Acknowledgment, Validation, and Replication
  - Phase 2 – Vulnerability Resolution with workarounds, patches, and fixes
  - Phase 3 – Responsible Disclosure and call to action

Types of Vulnerability Disclosure

- Full Disclosure
- Responsible Disclosure
- Public Disclosure
- Entitled Disclosure
- Critical Notification Plan (CNP)
- Partner Notification Plan (PNP)
- Phased Disclosure

Full Disclosure

- *(Wikipedia) In computer security, full disclosure means to disclose all the details of a security problem which are known. It is a philosophy of security management completely opposed to the idea of security through obscurity.*

- Usually means that all information about the vulnerability is made immediately public.

Responsible Disclosure

- *(Wikipedia) Some believe that in the absence of any public exploits for the problem, full and public disclosure should be preceded by disclosure of the vulnerability to the vendors or authors of the system. This private advance disclosure allows the vendor time to produce a fix or workaround.*

- Some vendors may choose to maintain a responsible disclosure stance in perpetuity. Exploit details are withheld from the customers as corporate confidential.

Public Disclosure

- Everyone on the Net has access to the details of the vulnerability and/or the Security Bulletin providing information about the vulnerability. This includes all customers of the vendor and all miscreants with an intent to do harm to those customers.

- Used by many vendors who have a broad customer base who may not be support customers.

Entitled Disclosure

- Security Bulletin only accessible it customers and partners of the vendor with a legal agreement.
- Variants of Responsible Disclosure:
  - Limit access to customer & partners
  - No broadcasting to the public, news, or security aliases.
  - No deniability – if asked, provide interested parties with the link to the Security Bulletin and the Title – but requires username/password for further details.

Critical Notification Plan (CNP)

- Where the undisclosed vulnerability poses a critical threat to critical infrastructure.
- For past dialog, please see
  - ftp://ftp-eng.cisco.com/cons/isp/security/CPN-Summit-2004/Paris-Sept-04/SE13-PSIRT-IOS-RELEASE-OPERATIONS-SECURITY-and-SP-OPERATIONS-v.1.pdf
- Ongoing problems with CNP:
  - What is critical infrastructure?
  - Who gets notified?
  - What are the metrics used for "critical" – where everyone believes their mission is "critical?"

Partner Notification Plan (PNP)

- PNP is a system to notify and prepare a vendor's channel partners before the announcement or publication of a vulnerability.
- Required if the vendor's ecosystem is prepared to support their customers.
- Contracts and NDAs are required to provide some check and consequence if the disclosure process is broken.
- Microsoft's **Coordinated Vulnerability Disclosure (CVD)** & **Microsoft Active Protections Program (MAPP)** are examples of PNP

Phased Disclosure

- Phased disclosure is a evolution of the responsible disclosure process – merging factors of the vulnerability's risk along with the operational requirements of core infrastructure.
- At times, the **operational risk** of rushed – unplanned upgrades is <u>greater</u> than the risk of a vulnerability moving to active exploit status.
- Disclosure is conducted in phases – notifying increasingly larger number of organizations – until the final phase of general public disclosure.

ISC's Security Vulnerability Disclosure Policy

ISC’s Security Vulnerability Disclosure Policy

- ISC has migrated away from a “entitled disclosure” process to a phased disclosure process.
- The phased disclosure process mixes ISC’s responsibility to critical **Internet infrastructure**, **our customers**, **our operating system partners**, **our Forum subscribers**, **our “ISC Inside” partners**, and our large deployment of software running on networks throughout the world.

Our Objectives

- The objective of ISC's phased disclosure is to provide the opportunity to upgrade within a reasonable maintenance window to minimize rushed action and operational anxiety.
  - We balance the risk of rushed upgrades beside the risk of the vulnerability.

- As an open source organization, we are working to have all our vulnerability management processes public.
  - This will allow the processes and procedures to be used as a reference model for the industry.

Five Phases

- Five phases to our Vulnerability Management Process:
  1. Finder’s Report, Acknowledgment, Validation, CVSS scoring, and Replication (TDD).
  2. Vulnerability Resolution with workarounds, patches, and fixes.
     - Drafting the Security Advisory. Obtaining the CVE number.
  3. Phased Disclosure
     - Interacting with infrastructure partners, security folks, vendors, customers.
  4. General Public Notification Phase
     - Reaching as many constituents as possible
  5. Postmortem Review

Two Types of Vulnerability Response

- At ISC, we follow two sorts of process in determining types of security emergency.
  1. Issues reported to ISC through private or secured channels are treated as “**Type I**” incidents (see “what to do if you find something”).
     - The normal Vulnerability Management Processes are used.
  2. **Live Operational Issues** or **Public Disclosure of vulnerability** are “**Type II**.”
     - Extremely compressed process, public notified as quickly as possible
     - Some lead time for root-ops and other key partners if possible

Note: *ISC treats all incidents impacting DNS operations at multiple sites as security issues until they are confirmed as non-malicious attacks.*

Version 1.1 Disclosure Phases

- **Phase One:** *ISC Forum subscribers, ISC software support customers, and DNS Root Operators (where applicable).*
  - Formal notice and pre-release code snapshot at least five business days in advance of the release of the public disclosure.
- **Phase Two:** *CSIRTs and other global security tracking organizations.*
  - Written notice of the disclosure ~24 hours before planned release of the public disclosure and code.

Version 1.1 Disclosure Phases

- **Phase Three:** *Vendors who package our code* into their operating systems, appliances, and products, receive written notice of the disclosure ~24 hours before planned release of the public disclosure and code.
  - Vendors who are Software Forum Members receive notification in Phase One.
- **Phase Four:** *General Public disclosure* of the vulnerability, and release of patched versions of all currently supported affected code.

Factors that Impact Phased Disclosure

- **Contractual Trust** (working non-disclosure) and **Operational Trust** (working discreetly through the remediation) is critical for a Phased Disclosure to work.
  - The chain of consequences of a disclosure leak impact the whole community.
  - This is why few vendors (software or hardware) use a phased disclosure approach. It requires more investment in time and effort to ensure that it works effectively.
  - Non-Disclosure agreements are included in ISC's Support, Service, and Forum contracts -- but other organizations require a NDA.

Factors that Impact Phased Disclosure

- Encrypted communications is required throughout the phased disclosure.
  - It takes time to exchange PGP keys (if keys are available).
  - Not all organizations or individuals use PGP
  - Not always easy to exchange keys

What’s Next?

- ISC continuously improves our Vulnerability Management and Disclosure Processes. Versions 1.2, 1.3, 1.4 (etc) will have:
  - Security Advisories in Multiple Languages – working with our partners (i.e. ccTLD colleagues, CSIRTs, Universities) and our international staff.
  - Phase 1 disclosure 7 days before the public release.
  - Integration of Vendor and Operating System Partners into the Phase 1 disclosure to have the packages ready to go on the General Disclosure Phase (T0). This is similar to Microsoft’s and ICASI’s Coordinated Vulnerability Disclosure.

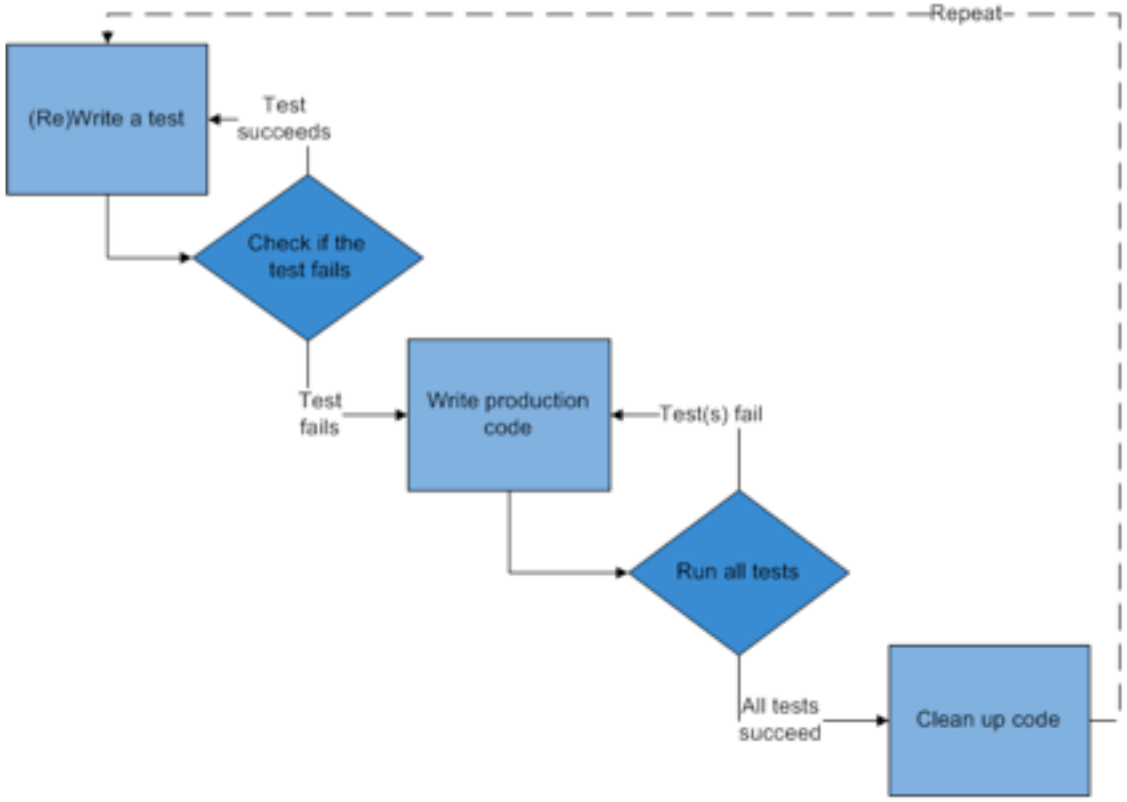
What’s Next (cont)?

- Work with National CSIRTs to provide secured disclosure sooner than 24 hours before public advisory.
- Work with global partners to prepare vendor specific software versions and local language notification at public disclosure.
- Briefing Calls and Webinars with our support customers & forum subscribers.
- First publication of our vulnerability management processes and procedures via our Knowledge
- Increase compliance with the Common Vulnerability Reporting Framework (CVRF)

Test Driven Development (TDD) and Vulnerability Disclosure

TDD and Vulnerabilities

- ISC uses Test Driven Development extensively as a key engineering quality process.
- Once we have validated & replicated the vulnerability, we then write a unit test.
- We then fix the code and verify using the test.
- When we get ready to release the code, we pull out the test so people will not know how to build an exploit.
- This unit test is a regression test. We need to find an appropriate time to put it back into the code.



Version 2.0

- In the future ISC will move to v2.0 of our Vulnerability Disclosure Process.
- The major change in 2.0 will be a public policy stating when the unit test/ regression test for the defect (vulnerability) will be integrated back into the code.
  - Operators ask us for this information for their own verification processes.
  - This could make it easier to build an exploit.

Prerequisites to Version 2.0

- ISC has a lot of work to do to prepare the our constituents for the impact of TDD in open source.
  - We need to have on-line training for our support customers, forum subscribers, and submitters.
  - We need to improve communications channel with our customers and the global community (i.e. let them know they should upgrade)
  - We need to interact with the FIRST community to review the impact this will have greater community.

Path to Version 2.0

- We're asking our support customers, forum subscribers, submitters, and global user community for feedback as we integrate TDD practices with our vulnerability disclosure process.
  - What do we need to prepare?
  - What do you need to prepare?
  - How might this impact your operations?
  - What is the appropriate time between the general disclosure and when we integrate the unit/regression test back into the code?

ISC’s Use of the Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS)

- CVSS provides ISC with an industry tool that improves our security risk, communications, and disclosure processes.
- It allows us to perform an initial risk assessment and dialog with the vulnerability’s finder to insure we apply the appropriate level of response.
- The CVSS Base Score is now included as part of our Security Advisory.

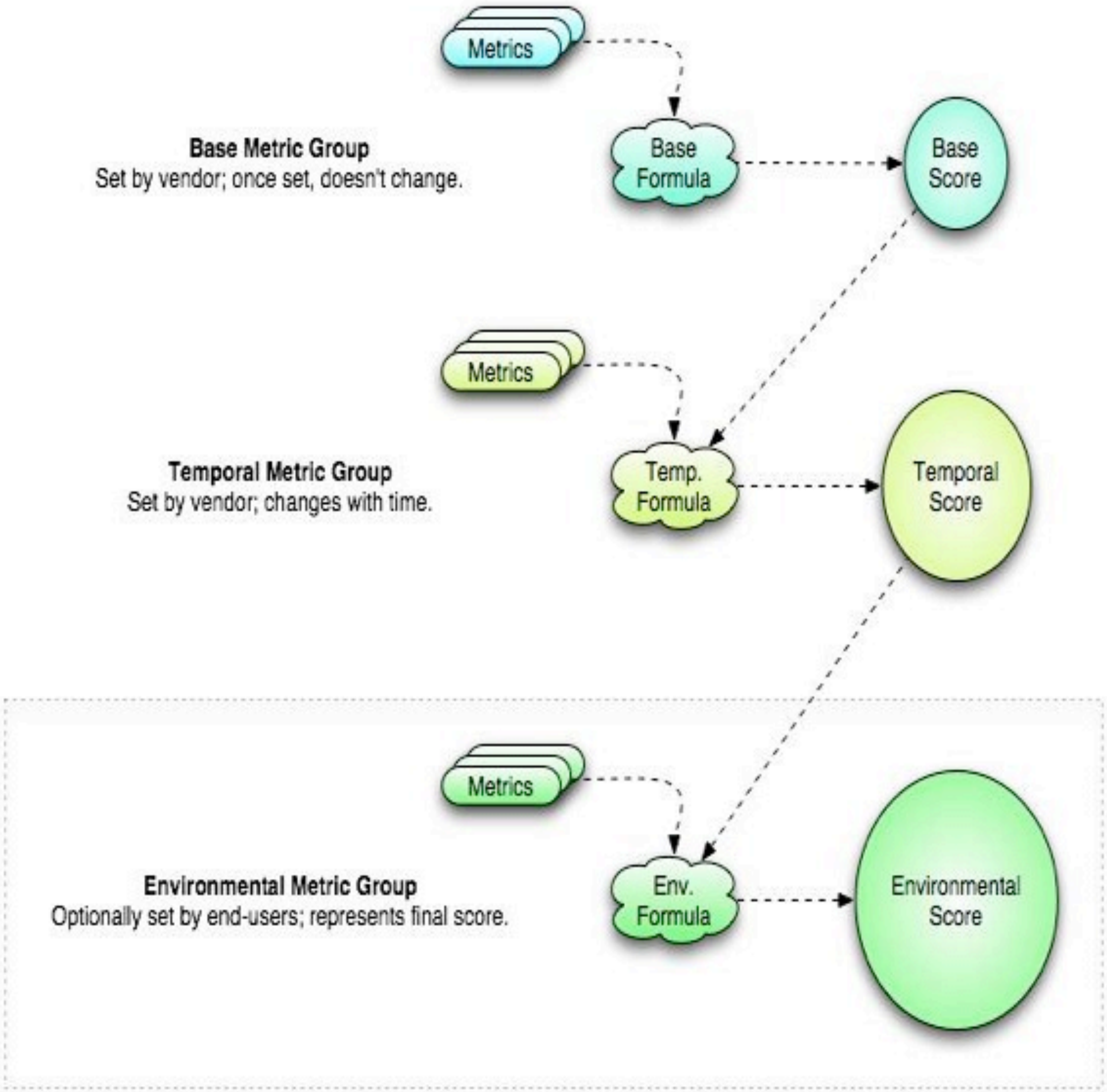
How does CVSS work?

- The Common Vulnerability Scoring System (CVSS) is a tool that allows two very different organizations to have a meaningful conversation about the risk a vulnerability can have on a network.
- CVSS uses metrics and formulas to yield a score that can be used to assess potential risk.

METRICS
+
FORMULAS
=
SCORE

Components of CVSS Score

- Base Score
  - Based on the parameters that are intrinsic to any given vulnerability that do not change over time
- Temporal Score
  - Based on the parameters of a vulnerability that change over time
- Environmental Score
  - Based on the parameters of a vulnerability that are specific to a user's environment


Metrics
Base Metric Group
Set by vendor; once set, doesn't change.
Base Formula
Base Score
Metrics
Temporal Metric Group
Set by vendor; changes with time.
Temp. Formula
Temporal Score
Metrics
Environmental Metric Group
Optionally set by end-users; represents final score.
Env. Formula
Environmental Score

CVSS is a Metric which drives action

- CVSS is used by CSIRT/SIRT Team for:
  - Consultation inside the organization on the risk
  - Setting priority of assigned Support Resources
  - Setting priority of assigned Engineering Resources
  - Determining which images will be fixed
  - Deciding when we would need a security advisory to drive upgrades and mitigations with our customers
    - cf. Security Notice, Security FYI, or ordinary KB article
  - Defining how to communicate risk to our customers

ISC CVSS Scoring

CVSS Base Score	Internal Description	Disclosure	Build Plan
8 - 10	**Critical & Catastrophic**	**Potential Critical Notification Process**	**Fix all images to cover the majority of deployed code (i.e. open EOL images.)**
7	**Critical**	**Security Advisory**	**Fix all Non-EOL Images**
5 - 6	**High**	**Security Advisory**	**Fix all Non-EOL Images**
3 - 4	**Medium**	**No Advisory**	**Fix all Non-EOL Images**
0 - 2	**Low**	**No Advisory**	**Just Fix it and Move Forward**

Questions

?

CVSS and CVRF References

- CVSS-SIG: http://www.first.org/cvss/
- CVSS v2 Complete Documentation:
  - http://www.first.org/cvss/cvss-guide.html
- NIST Interagency Report 7435:
  - http://csrc.nist.gov/publications/nistir/
- NIST NVD:
  - http://nvd.nist.gov/cvss.cfm?version=2
  - http://nvd.nist.gov/cvss.cfm?calculator&version=2
- Common Vulnerability Reporting Framework
  - www.icasi.org/docs/cvrf-whitepaper.pdf

Keeping in Contact

http://www.facebook.com/InternetSystemsConsortium

http://www.linkedin.com/company/internet-systems-consortium

http://twitter.com/ISCdotORG

ISC Resources

Knowledge Base articles about many things

http://deepthought.isc.org/

bind-announce for release notifications

http://lists.isc.org/mailman/listinfo/bind-announce

bind-users for community assistance

http://lists.isc.org/mailman/listinfo/bind-users

Thank you for your time.

www.isc.org