ISC's Vulnerability Management Process

Michael Graff mgraff@isc.org
Barry Greene bgreene@isc.org

Version 1.4

Thursday, February 2, 2012

About the Presenters

- Michael Graff
  - BIND 9 Engineering Manager
  - mgraff@isc.org
  - @skandragon

- Barry Greene
  - President
  - bgreene@isc.org

Agenda

- Update on CVE-2011-4313 - BIND 9 Resolver crashes after logging an error in query.c
- BIND 9 Engineering Design Notes
- ISC's Vulnerability Disclosure Policy – 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

Connect to ISC

- This presentation can be downloaded from the Webinar recording and from ISC's Knowledge Base: http://kb.isc.org
- ISC updates, presentations, and materials can be followed on:


Facebook - http://www.facebook.com/InternetSystemsConsortium


Twitter – ISCdotORG


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


RSS via our Website

Connect to ISC

- **ISC News Letter** – Get the quarterly ISC news letters, invitation to future webinars, information about the BIND/DHCP Events, and the 2012 ISC Summit.
  - https://www.isc.org/askisc (select ISC Newletter)
- **Subscribe to ISC project focused mailing list.** Sign up to your community of peers who all using the same ISC software.
  - https://lists.isc.org/mailman/listinfo
- Explore support contract, forum subscriptions, and ISC Organizational Membership:
  - www.isc.org

Update on CVE-2011-4313

Review CVE-2011-4313

- What happened?
  - Organizations across the Internet reported crashes interrupting service on BIND 9 nameservers performing recursive queries.
  - Affected servers crashed after logging an error in query.c with the following message:
  - INSIST(!dns_rdataset_isassociated(sigrdataset))
  - Multiple versions were reported being affected, including all currently supported release versions of ISC BIND 9.

- ISC investigated the root cause and produced patches which prevent the crash.
- The “time window” of the crash was limited and not repeated.

Review CVE-2011-4313

- ISC – working with REN-ISAC, the operational security community, and customers submitting logs, have traced to the root “trigger.”
- We have interviewed the organization(s) who were suspected triggers and validated that the trigger was a unforeseen operational interaction. Nothing was malicious.
- A previously unknown bug in BIND caused an internal inconsistency which lead to the crash.

Review CVE-2011-4313

- While the original trigger for this incident no longer exists, it is very possible that the same set of circumstances could be made to recur deliberately rather than accidentally.

- Therefore, ISC strongly recommends that those running vulnerable servers continue to update to a patched release of BIND.

- The CVSS Base Score remains at 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

Patch Details

- Versions affected:
  - BIND 9.0.x -> 9.6.x, 9.4-ESV->9.4-ESV-R5, 9.6-ESV->9.6-ESV-R5, 9.7.0->9.7.4, 9.8.0->9.8.1, 9.9.0a1->9.9.0b1
- Workarounds:
  - Recommendation is to patch -- but read on...
- Solution:
  - Patches mitigating the issue for all supported (i.e. no EOLed images) are available at:
  - https://www.isc.org/software/bind/981-p1
    https://www.isc.org/software/bind/974-p1
    https://www.isc.org/software/bind/96-esv-r5-p1
    https://www.isc.org/software/bind/94-esv-r5-p1

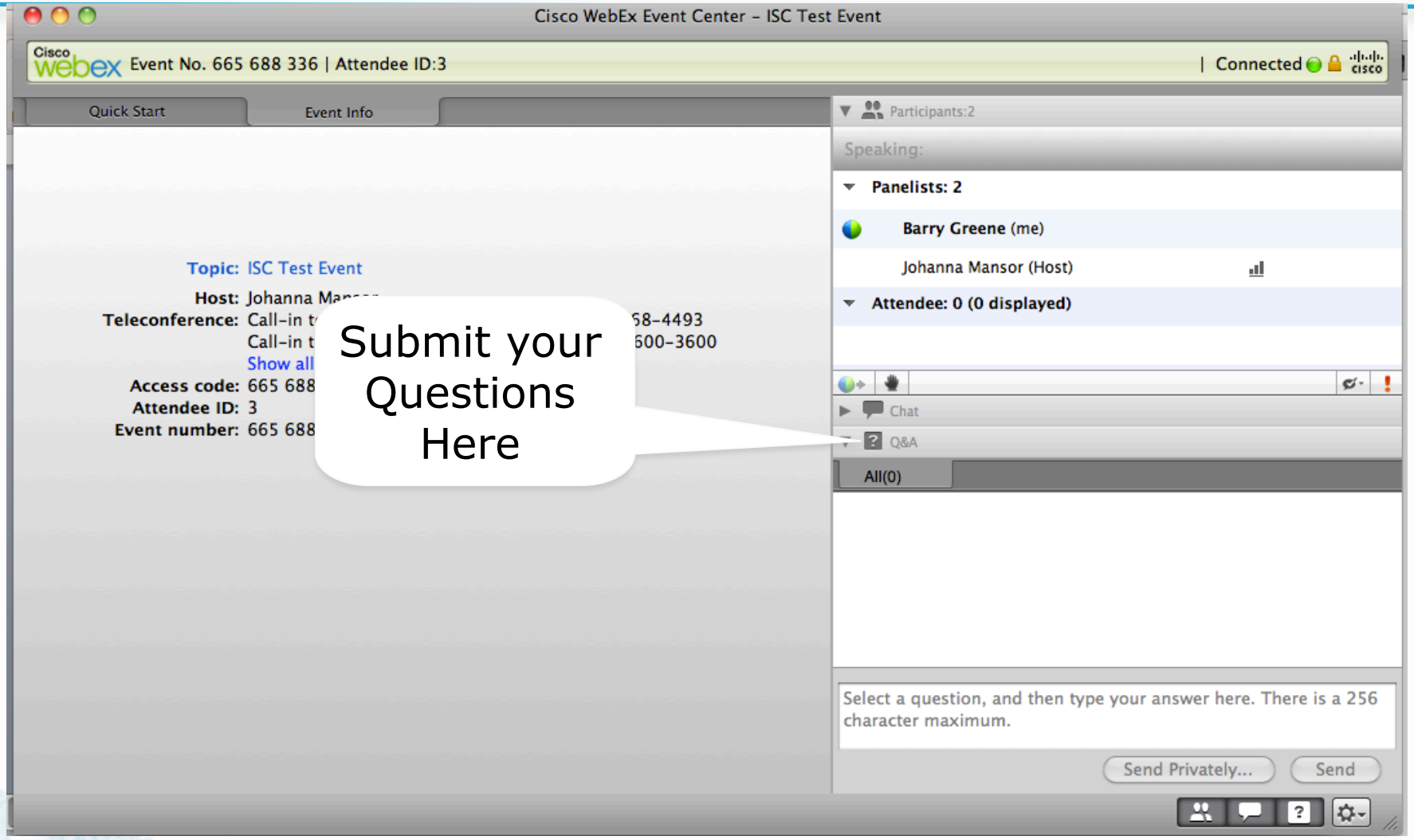
Workaround

- Only for purely recursive and forwarders
- Removes optional parts of responses
- Can cause more queries to be sent

```
options {
  minimal-responses yes;
};
```

- ... But you really should patch.

Pause for Questions



BIND 9 Engineering Design Notes

Detecting Defects

- BIND 9 detects abnormal situations
- BIND 9 detects programmer errors

- We try to react appropriately
- Sometimes, the best action is to crash

- BIND 10 is different, with other options

In this case…

- This CVE is related to internal data structures
- BIND 9 detected an abnormal situation
- Wasn't expected by the programmer

- The fix in this patch is to handle this edge case properly, without crashing

- A more complete fix will come later

Finding Defects, Old Style

- ISC is changing how we interact with defect finders

- Old style:
  - Gather information from finder
  - Write a fix
  - Add some tests if needed
  - Release

Finding Defects, New Style

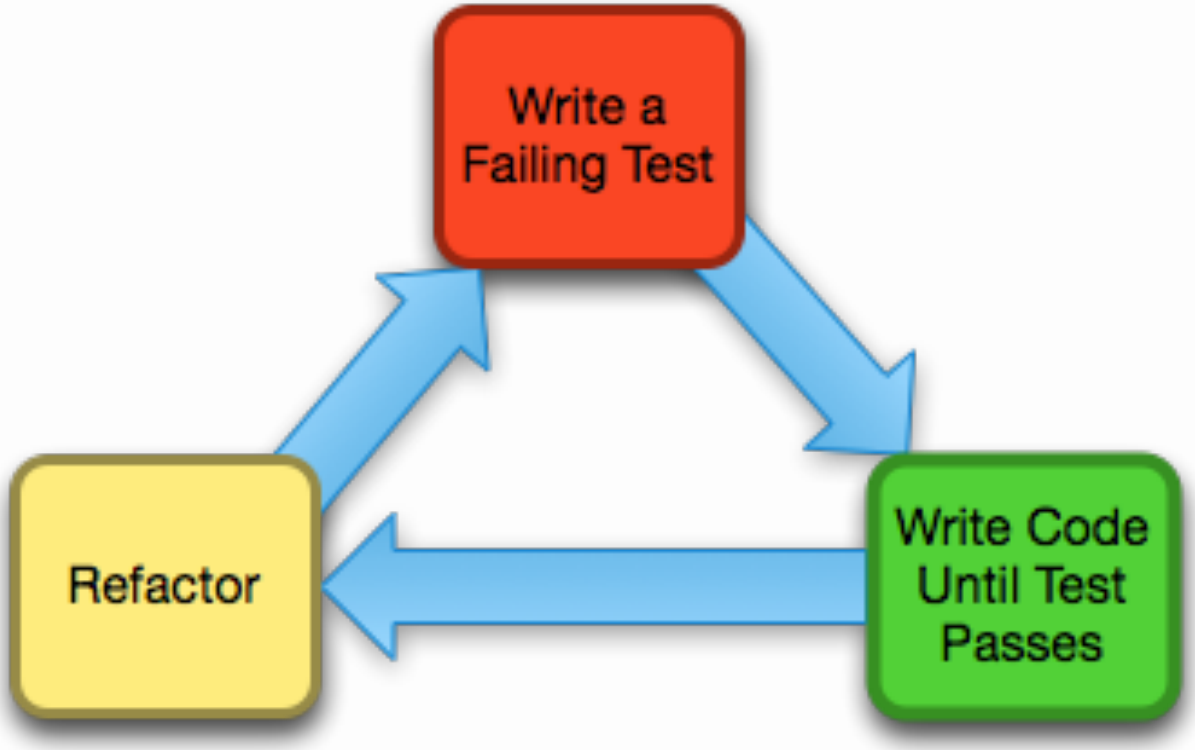
- New Style:
  - Interact with finder to understand
  - Write tests to identify flaw
  - Write the fix
  - Confirm the tests pass
  - Confirm fix with finder
  - Release using our phased disclosure policy

Test Driven Development

- ISC uses TDD

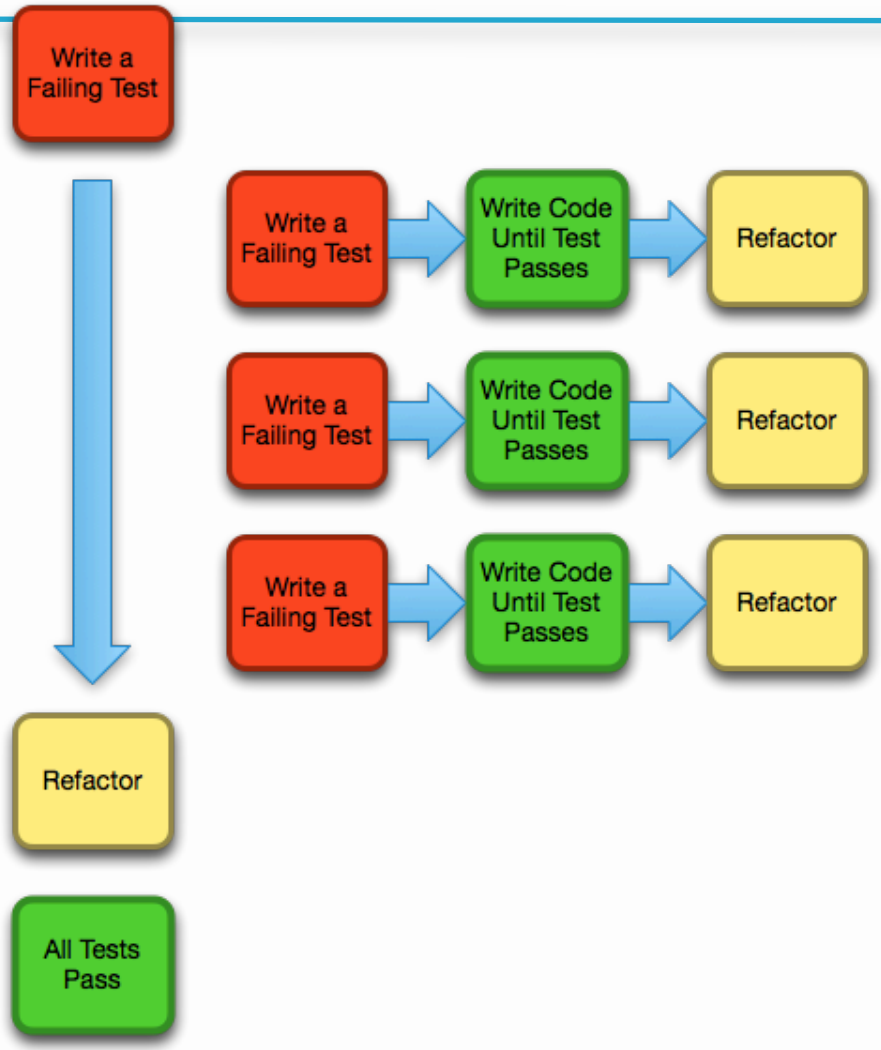
- General strategy of TDD:
  - Write a test that shows the failure
  - Write enough code to make the test pass
  - Refactor (clean up) code and test

TDD Cycle



Red, Green, Refactor.

TDD is Iterative

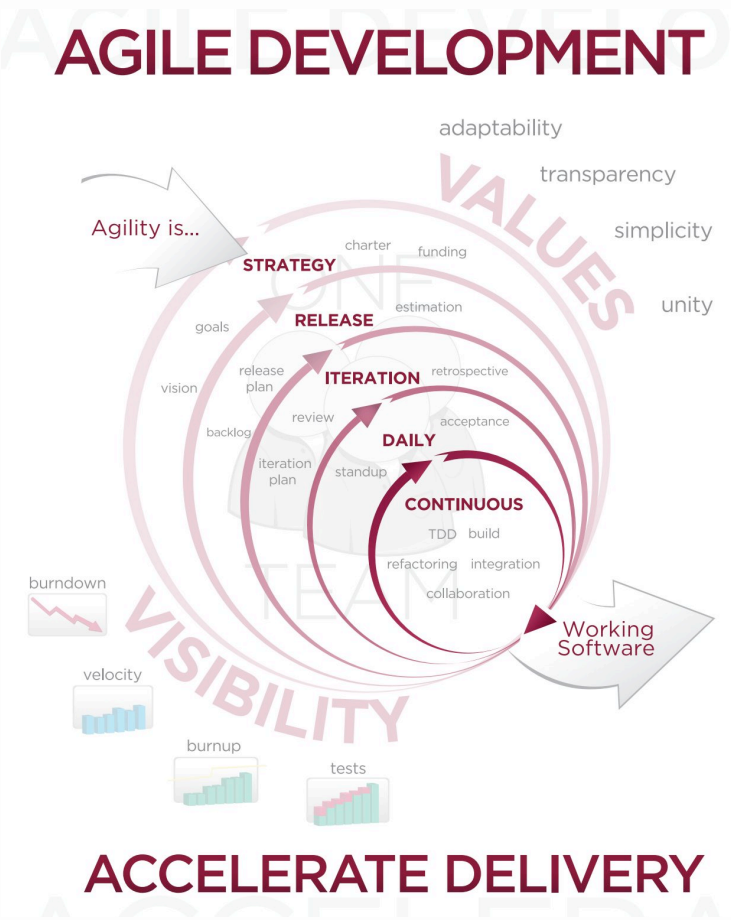


Why TDD?

- Ensures a regression test
- Higher assurance that the fix is...
  - Correct
  - Minimal
- Adding TDD to an existing product increases quality
- In BIND 9, there is a lot of legacy code
- In BIND 10, TDD is standard

Pause for Questions

- Start with Wikipedia for exploration into Agile and TDD ….
- http://en.wikipedia.org/wiki/Agile_software_development

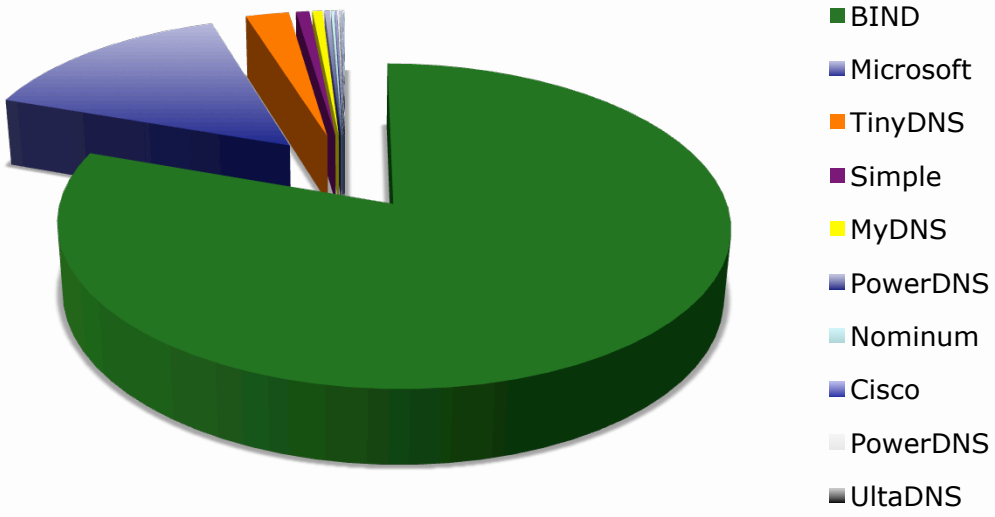


ISC's Vulnerability Management Principles

ISC's Role with in the Industry

Given ISC's role as the custodian of BIND, DHCP, and other Internet Critical Software, the massive adoption of BIND, & the critical dependency on DNS & DHCP which goes beyond the Internet to many aspects of telecommunications, **ISC has to manage all suspected vulnerabilities along the highest standards responsible disclosure.**

July 2011 *Internet Domain Survey* found 108937 DNS Servers



ISC's Vulnerability Management History

- Ad-Hock
- Situational
- "Friends and Family"

- Paying customers and forum members get early disclosure.
- All other constituents are notified during the general public disclosure.

- Successive layers of constituents, OS Teams, and critical vulnerability management teams are notified

Vulnerability Disclosure Community

Industry Processes

- ISC has adopted industry best practices for managing vulnerabilities. We are using these tools applying Agile principles, and working on open processes:

Common Vulnerability Scoring System (CVSS) – *used for risk assessment and a vehicle to come to a common risk consensus with the FINDer and Constituents.*

http://www.first.org/cvss

Common Vulnerabilities and Exposures (CVS) – *used by ISC to number our security advisories and provide a industry unique identifier (used through out the vulnerability test and compliance industry).*

http://cve.mitre.org/

Industry Processes

Common Vulnerability Reporting Framework (CVRF) v1.0 – Using the framework to update the information expressed in our security advisories.

The Role of the "FINDer"

What can the person or organization do when they find a vulnerability?

The Role of the FINDer

- The person or organization who finds the vulnerability is referred to as the "FINDer."
  - Other terms are used, but "FINDer" is more common today.
- The FINDer is the party who is in control over what is done with the vulnerability.
- The FINDer may choose to:
  - Inform the vendor or custodians of the software (if open source)
  - Contact a CSIRT Team
  - Tell their friends.
  - Announce at a security conference.
  - "Full Disclosure"
  - Publish in a journal
  - Sell the vulnerability to a security company
  - Sell the vulnerability to a criminal or other party
  - Do nothing (more common than you think).

FINDer "Realities"

- There is not much a vendor, government, or other party can do to stop a FINDer from choosing their disclosure path.
  - Law suits, legislation, and government action might work once, but only once.
  - AKA – 2004 and the TCP Window Size Disclosure
- Given this, a clear, publishes, and scalable procedure for vendors to cultivate trust and respect from the FINDers is prudent and beneficial.
  - BlueHat is one example.

ISC's FINDer Principles

- **Respond to the FINDer ASAP.** Let them know we have received the issue and are no working on it.
- **Ask the FINDer if they can work with our Vulnerability Management Processes.** Provide the FINDer with the pointer and the details.
- **Investigate the issue & ask for help if we cannot replicate.** Work toward replication and validation. Once replication is complete. Use CVSS to put a metric on the validation. If we cannot replication, ask the FINDer for help to build a valid replication. Honest humility of our limitations builds good will with many FINDers. We cannot know everything nor have the facilities to be able to replicate everything.

ISC's FINDer Principles

- **Share with the FINDer the CVSS score.** If they are not familiar with the CVSS score, brief them on how it works. Get confirmation on the CVSS Base score with the FINDer. This sets joint expectation on the priority that will be used to resolve the vulnerability. Share with the FINDer the organization's CVSS prioritization metrics.
- **Ask if the FINDer can help validate the FIX.** ISC validates the fix in two stages. First we write the Test Driven Development (TDD) for code for which we use TDD. Second we would write the fix to the code. We would share the fix with the FINDer to test to insure it fixes the code in their replication environment.

ISC's FINDer Principles

- **Share and Sync with the FINDer on the Vulnerability Disclosure Timetable.** Fixed code transitions the process to the vulnerability disclosure phase. We would work with the FINDer to insure they are in sync with our disclosure time table. We may need to brief the FINDer about the details of our phase disclosure process.
- **Notify the FINDer when ever there is a change to the vulnerability disclosure time table.** The FINDer might have their own disclosure work that is being worked in parallel.
- **Acknowledge the FINDer during the disclosure process.** We can acknowledge that we had good cooperation with a FINDer during the process. If the FINDer does not want to be named, we would *acknowledge the generous partnership of an anonymous FINDer and which to thank them.*

Vulnerability Disclosure Models

Approaches used to communicate to a vendor's constituents.

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 broad customers who may or may not be on support contracts.

Entitled Disclosure

- Security Bulletin and the details in that bulletin are only accessible by customers and partners of the vendor with an active agreement (support or partnership).
- Variant of Responsible Disclosure:
  - Limiting access to customer & partners
  - No broadcasting to the public, news, or security aliases.
  - No deniability – if asked, provide interesting parties with the link to the Security Bulletin and the Title – but requires username/password for further details.

Critical Notification Plan (CNP)

- A type of Security Alert 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
- On going problems with CNP:
  - What is critical infrastructure?
  - Who get notified?
  - What are the metrics used for “critical” – where everyone believes their mission is “critical?”

Partner Notification Plan (PNP)

- Also call Microsoft's **Coordinated Vulnerability Disclosure (CVD)** & **Microsoft Active Protections Program (MAPP)** are examples of 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.

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 to apply remediation within planned and rational maintenance windows.
- At times, the **operational risk** of rushed – unplanned upgrades is greater than the risk of a vulnerability moving to active exploit status.
- Disclosure is conducted in phases – notify successive great larger number of organizations for action – 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 phase 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 constituents networks through out the world.
- The objective of the phase disclosure is to provide the opportunity to upgrade within a reasonable maintenance window to minimize rushed action.

Our Objective

- The objective of the phase disclosure is to provide the opportunity to upgrade within a reasonable maintenance window to minimize rushed action.
  - We balance the risk of rushed upgrades beside the risk of the vulnerability.
- Given that we're an open source based organization, we are working to have all our vulnerability management processes published.
  - This will allow the processes and procedures to be used as a reference model for the industry.

The Macro Phases

- ISC has five major phases to our Vulnerability Management Process:

1. "FINDer's" Vulnerability Reporting, Acknowledgment, Validation, CVSS scoring, and Replication with a Test Driven Development (TDD) Unit Test.
2. Vulnerability Resolution with workarounds, patches, and fixes. Crafting the Security Advisory. Obtaining the CVE.
3. Phased Disclosure – Interacting with the Constituents.
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.
- Issues reported to ISC and **not live** on the Internet are treated as "**Type I**" incidents.
  - The normal Vulnerability Management Processes are uses.
- **Live Operation Issues** or **Public Disclosure of issues** are "**Type II**."
  - Everything is compressed to real time.
  - Communications to the "phased disclosure community" is near real time. General public is via our Security Advisory.

Note: *ISC treats all "incidents" impacting DNS operations at multiple sites as a Security Issue until it can be positively confirmed as not malicious.*

Version 1.1 Disclosure Phases

- **Phase One:** Authorized ISC Software Forum subscribers, all ISC software support customers, and DNS Root Operators.
  - They receive formal notice and pre-release code snapshot as far in advance as possible.
  - This is usually between at lease five business days in advance of the release of the public disclosure and code.
- **Phase Two:** CSIRTs and other global security tracking organizations.
  - Receive 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 Phase 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 phase disclosure approach. It requires more investment in time and effort insure in works effectively.
  - Non-Disclosure agreements on are part of ISC's Support, Service, and Forum contracts --- but other organizations require a NDA.

Factors that Impact Phase Disclosure

- Encrypted communications is required through the phase disclosure.
  - It takes time to exchange PGP keys (if keys are available).

What's Next?

- ISC is continuously improving our Vulnerability Management and Disclosure Processes. Version 1.2, 1.3, 1.4 (etc) will have new functions:
  - Security Advisories in Multiple Languages – working with our partners (i.e. like JPRS) and our staff (who reside in many parts of the planet), we are able to reach out with security advisories in multiple languages.
  - Moving the Phase 1 disclosure to 7 days before the general public release.
  - Integration 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.

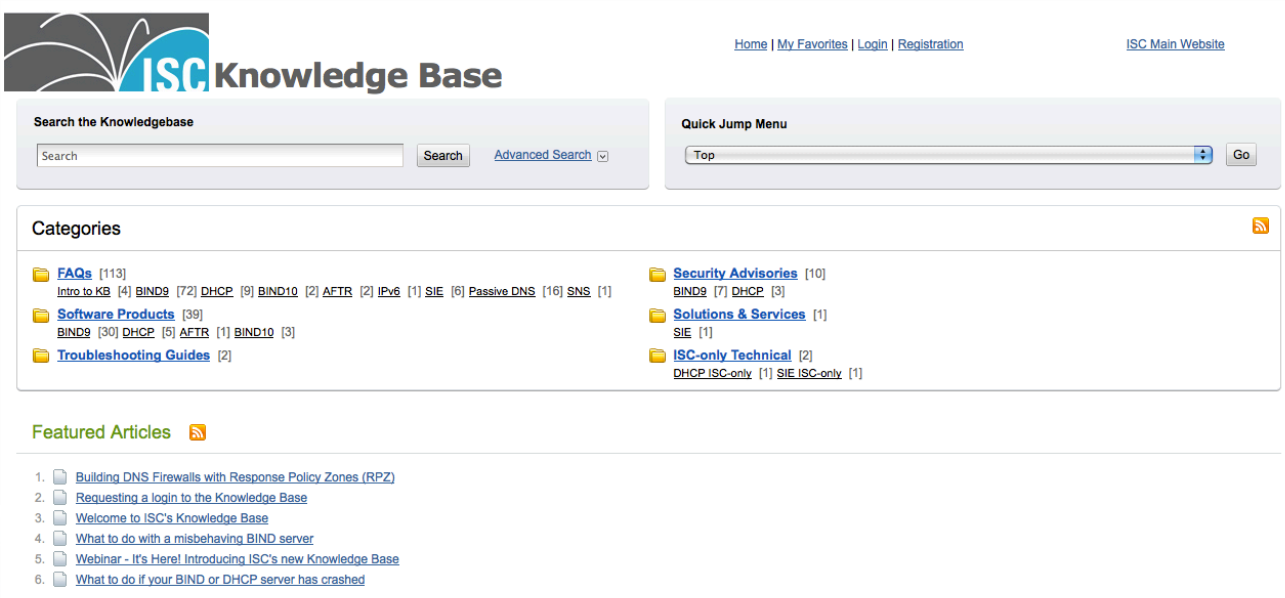
What's Next (cont)?

- Work with several key National CSIRTs to disclosure sooner than 24 hours before and prepare software and local language notification.
- Briefing Calls and Webinars with our support customers & forum subscribers.
- First publication of our vulnerability management processes and procedures via our Knowledge Base.
- Integrating vulnerability test and audit community into the process.
- Using ISC's Knowledge Base (http://kb.isc.org) as the authoritative source for ISC's security advisories, vulnerability management processes, and vulnerability management policies.

Pause for Questions

- Please submit your questions ….

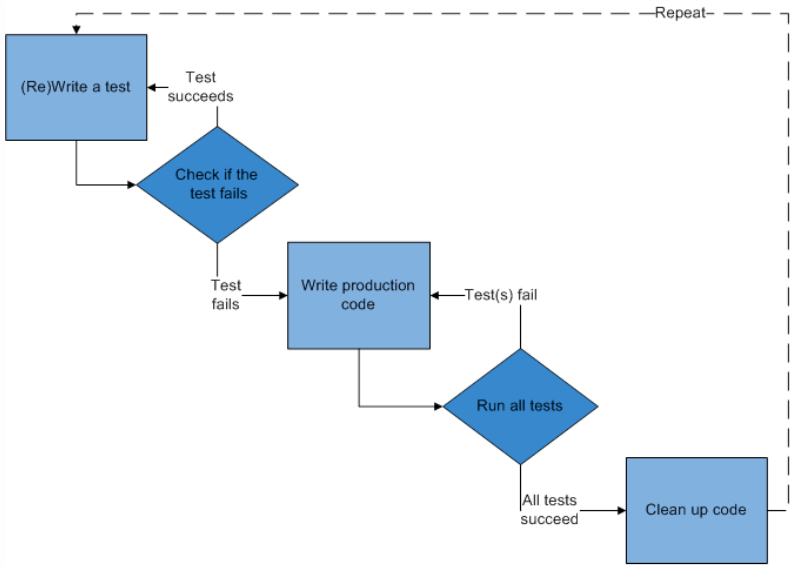
- In the mean time, please visit our ISC Knowledge Base at http://kb.isc.org



Test Driven Development (TDD) and Vulnerability Disclosure

TDD and Vulnerabilities

- Today, once we have validated & replicated the vulnerability, we then write a unit test in the code to insure we know what to fix.
- We then fix the code leaving the unit test in the code.
- 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

- Some time in the future ISC will move to version 2.0 of our Vulnerability Disclosure Process.
- The major change will be a public policy stating when the unit test/regression test for the defect (vulnerability) will be integrated back into the code.
- The will make it easier to build an exploit.

Prerequisites to Version 2.0

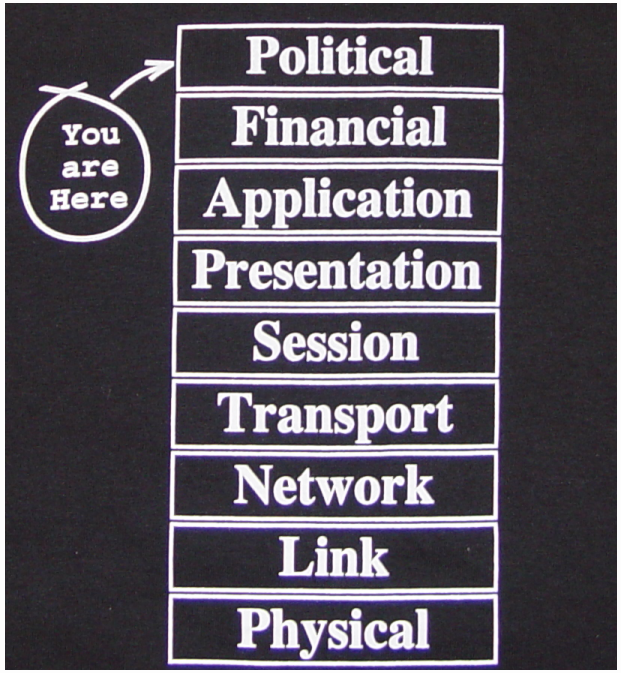
- ISC has a lot of work to do to prepare the our constituents for the impact of TDD in open source.
  - We need to have effective on-line training for our support customers, forum subscribers, and submitters.
  - We need to reach out to more of our constituents to insure we have a proper communications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

Ask for the path to Version 2.0

- We're asking our support customers, forum subscribers, submitters, and other constituents for feedback as we journey TDD's integration 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?

Pause for Questions

- Please submit your questions.



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 no 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 have a meaningful conversation about the risk a vulnerability can have on a network.
- CVSS used metrics and formulas to yield a score.
- That score is used to translate potential risk.

Components of CVSS Score

- Base Score

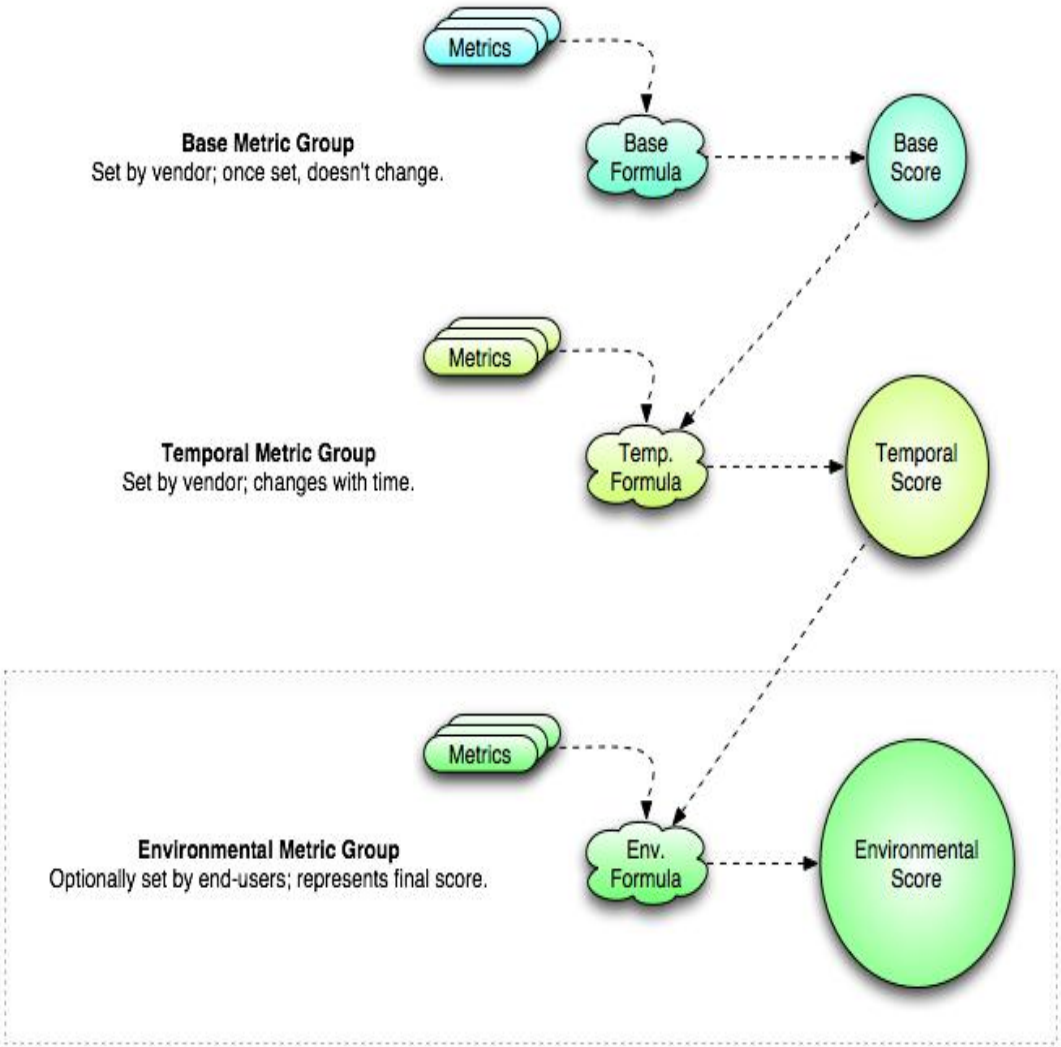
  Based on the parameter
  vulnerability that do not

- Temporal Score

  Based on the parameter
  time

- Environmental Score

  Based on the parameter
  user's environment



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 to use 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

CVSS Scoring ISC

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

CVSS References and Links

- 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

Questions?

security-officer@isc.org

How to Connect to ISC's Vulnerability Disclosure Process

Step 1- Connect to ISC

- ISC needs a way to communicate with your organization so that you will know when the general public vulnerability disclosure is posted.
  - **Connect to ISC's Mailing list.**
  - **Connect to our New Letter List** (https://www.isc.org/askisc)
  - **Connect via Social Media**
- Converse with ISC if these communications channels are not working.
  - We are looking for suggestions to connect to as many of our constituents as possible.
  - E-mail security-officer@isc.org with suggestions.
  - Submit suggestion via https://www.isc.org/askisc

Step 2 – Software Support Contract

- All software support customers for a product are included as part of the Phased Vulnerability Disclosure process.
  - The goal is to prepare our customers and upgrade within a rational maintenance window before the general public disclosure.
- ISC has a range of software support options to fit the requirements of many different organizations.
- Our support customers range from the largest service providers on the planet to small enterprises to Universities, to government networks, to critical infrastructure providers.

https://www.isc.org/support

Option A – Forum Subscription

- Some organizations have highly skilled engineers who actively interact with ISC's engineers.
  - These organizations don't need software support, but want to support ISC's work, the community's work, and stay connected.
  - Forum subscriptions are the means for these organizations to support the cause and stay connected.
- All Forum subscribers for a specific project are part of the Phased Vulnerability Disclosure Process. The goal is to help them prepare and upgrade within a rational maintenance window before general public disclosure.

https://www.isc.org/forums

Option B – Organizational Membership

- ISC's Organizational Members invest in the future of Internet Critical Open Source software, services, and infrastructure that are essential to a thriving Internet.
- All of ISC's organizational members are part of the Phase Vulnerability Disclosure process.
- Organizational members are part of the Technology Advisory Council are also part of the policy update and review for how ISC manages vulnerabilities.

https://www.isc.org/forums

Option C – National CSIRT Team

- Please contact ISC @ security-officer@isc.org
- ISC will work to integration your National CSIRT Team with the Phased Vulnerability Disclosure Process.
- Our goal is to enlist National CSIRT Teams to communicate to their constituents when ever there is a ISC security issue. This means we time to allow the National CISRT Team to prepare.

Option D – Operating System Team

- Please contact ISC @ security-officer@isc.org
- Or goal is to have packages ready for as many of the operating systems as possible before the general public disclosure.
- Deep dialog will help build processes that will allow us to meet this goal.

Don't get Caught Off Guard with Old BIND!

- Get Professional Support to help you upgrade BIND!
  - http://www.isc.org/getbindsupport
- Special Offer Software Support & Consulting Deal!
  - Take advantage of this special deal that combines 6 months of Basic Support & 8 hours of Expert Consulting to get your organization started with BIND support, have enough support time to get your systems upgraded, and convince management to budget for critical DNS infrastructure support.
- Webinar Special Discount!
  - ISC will E-mail all participants after the webinar. If you did not get or cannot wait, E-mail to sales@isc.org


THANK YOU