Coordinated Vulnerability Disclosure Reporting at ICANN

Version 2.0
Updated 5 August 2013

Table of Contents

This document describes the basic principles of Coordinated Vulnerability Disclosure Reporting as practiced by the Internet Corporation for Assigned Names and Numbers (ICANN).

Coordinated Vulnerability Disclosure refers to a reporting methodology where a party ("reporter") privately discloses information relating to a discovered vulnerability to a product vendor or service provider ("affected party") and allows the affected party time to investigate the claim, and identify and test a remedy or recourse before coordinating the release of a public disclosure of the vulnerability with the reporter.

Coordinated disclosures rely on private communications between reporter and affected parties during vulnerability investigations to limit risk to or prevent harm to third parties should the vulnerability be made public before remedies can be identified. Reporters agree to terms of Coordinated Vulnerability Disclosures with the expectation that the affected parties will seek a remedy when notified. All parties to the disclosure generally agree to refrain from disclosing the vulnerability to the public until a remedy is identified and tested or until the threat is considered

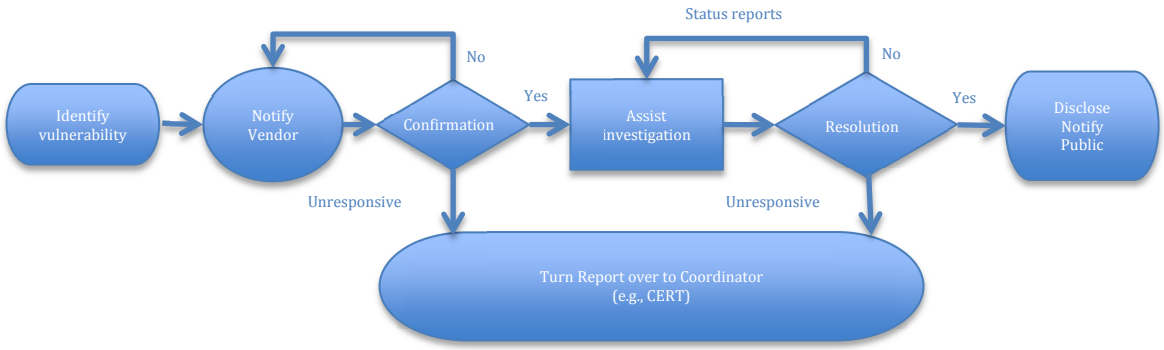
contained. It should be noted that while reporters and affected parties typically work in good faith, a reporter may choose to disclose a vulnerability when reasonable attempts to coordinate disclosure with an affected party are exhausted and the reporter is under no (legal) obligation not to disclose.

The methodology ICANN describes here for vulnerability reporting also applies to reporting threats to the security, stability, or resiliency of Internet identifier systems.

Under this methodology, a reporter may also give notice of a vulnerability or threat through a *coordinator* who is trusted by all parties to report directly and exclusively to the product vendor or services provider, such as a national computer emergency response team (CERT). ICANN explains how it acts as reporter, affected party, or coordinator.

Illustration of a Typical Coordinated Disclosure Process

Figure 1 illustrates the roles and relationships of parties typically involved in a coordinated disclosure.



Commitment

ICANN is publishing this reporting process within ICANN's role and remit to facilitate the security, stability, and resiliency of the Internet's unique identifier systems through coordination and collaboration. Visitors and users of ICANN websites, systems and services rely on ICANN to protect the data and services within the systems used by the community and organization. The security of the identifier systems, data and services is a responsibility ICANN takes seriously.

ICANN is committed to protect these from security threats and welcomes responsible and timely reports of any vulnerabilities discovered on ICANN websites, platforms, or processes. ICANN welcomes responsibly coordinated reports of vulnerabilities, and ICANN will collaborate with reporting parties to fix vulnerabilities or mitigate threats. Please note however that this document does not

give permission to anyone to break any law or to access any non-public data or systems maintained by ICANN. We expect reporters to abide by the following terms, which we believe are consistent with Coordinated Disclosure Reporting:

- Reporters will refrain from performing testing against ICANN's website, platforms, or services that would result in a disruption or denial of service.
- Reporters agree to privately share details of suspected vulnerabilities to our website or platforms, or threats to Internet identifier systems.

We intend to abide by these same terms when circumstances call for ICANN to serve as a coordinator or reporter.

Certain vulnerabilities – for example, where the consequences of an event may (indirectly) affect parties too numerous to contact directly, or where the potential for DNS service interruption is imminent or high – may require activation of broader crisis management handling measures within ICANN (including threat analysis, assessment of the potential for harm and estimation of the targeted assets or populations) and in coordination with a wider set of stakeholders (e.g., international, inter-governmental). This crisis management process is referenced in this document, but is a separate process, involving coordination with ICANN Communications and other departments as necessary, depending on the situation.

Reporting Process: ICANN as Affected Party

Notification and Report Submission

Reports of vulnerabilities found in ICANN's websites, platforms, or services, or threats against identifier systems should be submitted by electronic mail to < disclosure@icann.org>. For private, secure reporting we recommend that reporters use PGP or S/MIME. For the latest keys and fingerprints please visit https://www.icann.org/security/

Reporters should include as much of the following documentation as possible in a vulnerability or threat report:

- A summary of the vulnerability or threat,
- Technical details,
- Where applicable, a description of how to reproduce the vulnerability,
- The reporter's analysis and perceived severity of the vulnerability or threat, and
- Any additional information that may assist ICANN in investigating the matter.

ICANN will accept reports if cryptographically protected electronic mail is not available to the reporter; in such circumstances, however, the reporter should refrain from submitting vulnerability or threat documentation and instead only submit an email notification to ICANN to determine whether it is necessary to employ an alternative means to securely transmit technical details or other sensitive information.

If you are unable to contact ICANN using electronic mail, please contact us by telephone at +1 310 301 5800. Indicate that you are calling in regard to an Internet security matter or imminent threats and ask to be connected to ICANN's incident response officer.

Confirmation and tracking

ICANN will, within one business day, confirm receipt of the notification by email and assign a tracking identifier. Future correspondence between the reporter and ICANN, including status reports from ICANN, should reference this identifier. ICANN is a non-profit public benefit organization and is not in a position to offer cash awards to reporters, but ICANN would ordinarily be willing to publicly recognize and thank any responsible reporters of vulnerabilities or threats.

Validation and Status Reporting

ICANN will investigate the reported vulnerability or threat and provide the reporter with an initial assessment or estimated time for resolution within two weeks. ICANN will issue subsequent status reports as it continues to investigate progresses to inform the reporter of changes to the estimated time for resolution, i.e., when it expects to conclude the investigation, remedy the vulnerability, or report that the threat is considered contained. ICANN asks that reporters allow for sufficient time to fully investigate and resolve, especially in circumstances where ICANN has a coordinator role. Vulnerability reporters should refrain from publicly disclosing the vulnerability, threat or methods to reproduce (such as exploit code) while ICANN investigates the claim.

Resolution and Release

ICANN will notify the reporter when it has remedied the vulnerability or when it determines that the threat is contained. ICANN will have prepared a public release describing the issue and its resolution. We will share this with the reporter so that the parties can coordinate the disclosure of the vulnerability, its remedy, or the containment of the threat to the public.

Reporting Process: ICANN as Reporter

Notification and Report Submission

ICANN's preferred method of reporting vulnerabilities is cryptographically protected email to a designated vulnerability contact published by the affected. In a secure vulnerability notification, ICANN will attempt to provide:

- A summary of the vulnerability or threat,
- Technical details,
- Where applicable, a description of how to reproduce the vulnerability,
- ICANN's analysis and perceived severity of the vulnerability or threat, and
- Any additional information that may assist the affected vendor in investigating the matter.

Where secure email to a designated contact cannot be identified, ICANN will make reasonable efforts to obtain email or other contact information through other public resources, such as the administrative contact of the affected party's domain name registration record, social media contacts, alternate channels, or a coordinator such as a national CERT. In these cases, ICANN will notify the affected party but will wait for (secure) handling instructions from the affected party before submitting a detailed vulnerability report.

Confirmation and tracking

Depending on our assessment of the severity of the vulnerability or threat, ICANN will wait for one to ten days for confirmation of the affected party's receipt of its vulnerability notification. Upon confirmation, ICANN will provide documentation (if not submitted through a secure notification email), and will refrain from publicly disclosing the vulnerability, threat or methods to reproduce (such as exploit code) while the affected party investigates the claim.

Where the affected party fails to respond after reasonable efforts to contact have been exhausted, ICANN will attempt to contact the affected party through other channels or coordinators. If all reasonable attempts to contact the affected party fail, or if the vulnerability ICANN has attempted to report becomes publicly known, ICANN will consult with trusted parties such as a national CERT to determine an appropriate and responsible disclosure.

Validation and Status Reporting

ICANN will assist an affected party during its investigation of a reported vulnerability. We ask that affected parties provide an estimated time for resolution as well as progress or status reports during the investigation. ICANN will make

reasonable efforts to assist affected parties with testing to verify a remediation the vendor proposes to release.

Resolution and Release

Affected parties notified by ICANN of a vulnerability should inform ICANN when the vulnerability is remedied or when it is determined that the threat identified is contained. Affected parties should try and coordinate any public release describing the issue and its resolution. Where appropriate, ICANN will make a public disclosure through its own communications channels.

ICANN as a Vulnerability Coordinator

Under certain circumstances – particularly where a threat to the security, stability, or resiliency of Internet number systems or global DNS operations is identified – ICANN may be contacted to assist in a vulnerability investigation or threat response. In such circumstances, ICANN will confirm that all parties trust ICANN to act as coordinator. During this confirmation period, ICANN will (i) facilitate communications (i.e., introduce parties, provide vulnerability, abuse, or threat response point of contact information) and (ii) privately disclose only such information relating to the threat as is necessary for affected parties to assess whether they wish to have ICANN coordinate the investigation or response, or whether the parties will proceed with the investigation or response directly (without ICANN participation).

If ICANN is asked to coordinate, we will ask reporters to follow the guidelines described under Reporting Process: ICANN as Accepting Party. We will assist reporters in determining how to share information and if appropriate, assist in identifying affected parties (for example, there may be circumstances where ICANN may be able to identify other parties affected by the vulnerability or threat than those identified by the reporter). ICANN will follow the guidelines described under Reporting Process: ICANN as Reporting Party, privately share information with affected parties, and continue to coordinate and support investigation or response activities through to and including public release.

Reference: Other Coordinated Vulnerability Disclosure Policies

Below is a list of disclosure policies ICANN consulted in composing our Coordinated Vulnerability Disclosure Guidelines:

CERT/CC Vulnerability Disclosure,
http://www.cert.org/kb/vul_disclosure.html
EngineYard Responsible Disclosure Policy,
https://www.engineyard.com/legal/responsible-disclosure-policy
Google: Rebooting Responsible Disclosure,
http://googleonlinesecurity.blogspot.com/2010/07/rebooting-responsible-disclosure-focus.html
Microsoft Security Response Center: Coordinated Vulnerability Disclosure,
http://www.microsoft.com/security/msrc/report/disclosure.aspx
Secunia Vulnerability Disclosure,
http://secunia.com/community/research/policy/
SoundCloud Responsible Disclosure,
http://help.soundcloud.com/customer/portal/articles/439715-responsible-disclosure

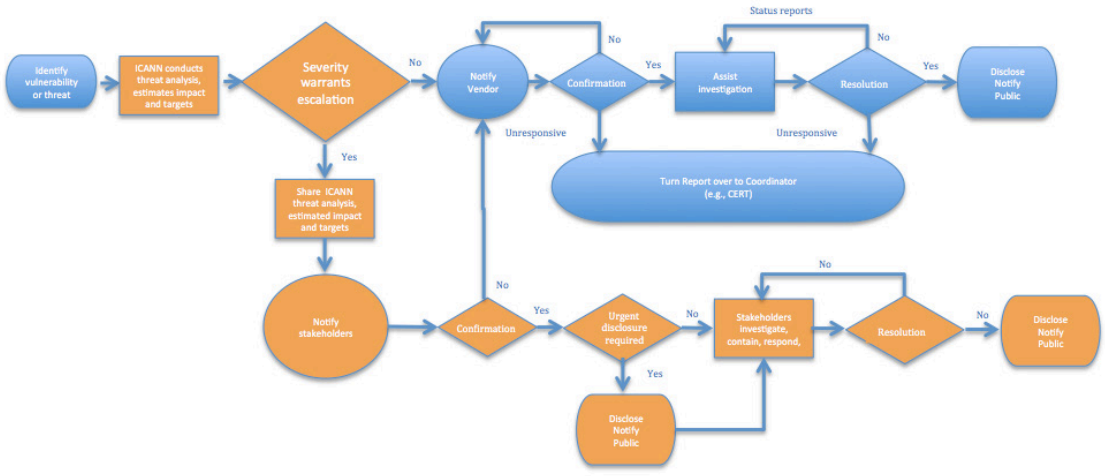
Emergency Coordination & Crisis Management

If a vulnerability or event requires activation of broader crisis management handling within ICANN and with other stakeholders, ICANN will follow its emergency coordination and crisis management processes. This is a separate but related process from the Coordinated Vulnerability Disclosure.

For top-level domain name issues, ICANN has an emergency escalation process described in Specification 10 of the generic top-level domain name Registry Agreement (see http://newgtlds.icann.org/en/applicants/agb/agreement-approved-02jul13-en.pdf). The process provides for monitoring of TLD registry operators for service level agreement performance. In the event that emergency escalation occurs, electronic (email or SMS) and or voice contact notification will be sent to the impacted registry operator's emergency operations department with detailed information concerning the issue being escalated. If necessary, Emergency Backend Registry Operators (EBEROs) may be utilized (http://www.icann.org/en/resources/registries/ebero/faqs).

For vulnerabilities that ICANN may activate an internal crisis management team, participants from ICANN's Security, Communications and other departments will confer and make a determination on whether to trigger the broader crisis management process. In the event that this process is activated, it will be managed separately from the Coordinated Vulnerability Disclosure process outlined in this document.

The relationship between the emergency coordination and crisis management process and coordinated vulnerability disclosure process is illustrated in Figure 2:



When ICANN receives information or notice of a vulnerability or threat, it will conduct a threat analysis to assess the nature and severity of the threat and will attempt to identify the assets or targets under threat and estimate the impact (and

risk) if the threat were to be manifested in a security event. If ICANN determines that the threat is real and imminent or severe enough to warrant escalation beyond parties directly affected by a vulnerability (e.g., software vendor or registry operator that uses the software), ICANN will share its threat assessment with stakeholders ICANN determines are either directly under threat, whose assistance is required to mitigate the threat, or whose assistance is required to notify others directly or indirectly under threat; for example, international government agencies, security or engineering communities, or private actors whose awareness or cooperation are needed to respond to the threat (such as an operator of a global and public resolver service).

Working in cooperation with the notified stakeholders, ICANN would seek confirmation that its threat assessment is correct. If stakeholders conclude that the threat is not severe, then ICANN will proceed as a coordinator in its vulnerability disclosure process.

If stakeholders concur with ICANN's threat assessment, ICANN and the stakeholders will determine if the threat warrants immediate disclosure and to whom (e.g., a public notification). ICANN and the stakeholders will collaborate to investigate, implement a readiness plan (to avert or contain threat not yet materialized), or respond (mitigate) to a security event.

At such time as the threat is averted or contained, or the security event is resolved, ICANN and the stakeholders will determine what notification is necessary. (Note: while not depicted in the flow diagram, ICANN and the stakeholders may choose at any time during their investigation or response to issue notices or progress reports, or they may decide that additional stakeholders should be contacted and asked to cooperate or collaborate.)