Guidance on Reporting Protocol Vulnerabilities to the IETF

The IETF recognizes that security vulnerabilities will be discovered in IETF protocols and welcomes their critical evaluation by researchers. Such research keeps the Internet safe. This page is intended to guide researchers in navigating the IETF to disclose and remediate these vulnerabilities.

Scope

The IETF is a standards development organization that publishes RFCs that describe Internet protocols and specifications. Internet-Drafts (I-Ds) are working documents used in the creation of RFCs. RFCs and I-Ds are collectively referred to as documents. While documents include an occasional reference or example source code, the IETF does not build or maintain implementations of protocols.

Design vulnerabilities or security issues with operational practices described in IETF documents can be addressed in the IETF. Implementation or configuration vulnerabilities in products, open source projects, or services that may implement these documents need to be addressed by their corresponding vendor. The IETF does not have a formal means to reach these parties.

Additionally, the IETF does not certify conformance of products to its published documents.

Vulnerabilities in any infrastructure and services that support the IETF, IRTF and IAB (such as those associated with the ietf.org, iab.org, irtf.org and rfc-editor.org domains) are the responsibility of the IETF Administration LLC who has their own vulnerability disclosure policy.

Transparency in the IETF

New protocol work and associated maintenance of published protocol specifications in the IETF is done through an open and transparent process. Issues are discussed on working group mailing lists and meetings which are public; and intermediate updates to documents (Internet-Drafts) as well as their final version (RFC) are also publicly available. Additionally, all posts to IETF mailing lists are considered an IETF Contribution per the IETF Intellectual Property Agreement.

The IETF standards process does not support private disclosure and remediation. If the severity or complexity of the vulnerability necessitates confidentiality, consider engaging a Computer Security Incident Response Team (CSIRT) for coordinated vulnerability disclosure. Additionally, privately contacting document authors or working group chairs can also be used to help assess the issue (See Activity #7 of Figure 1). All mail sent to IETF Working Group mailing lists is public.

Expectations from the IETF

The IETF values your critical analysis of its work. What the IETF will do with your vulnerability report, depends on the type of document where the issue is found; the severity of the issue; the complexity of the mitigation; and the maturity of the document in question.

- *For published RFCs (files named RFC####)*, these are completed, community reviewed documents. If the working group that produced the RFC is still active, it will work to vet the issue with you and decide the appropriate way to address the issue. If confirmed, the vulnerability might be addressed via an errata, an updated protocol specification document, or an entire new document to handle the issue. For closed working groups, the severity of the issue will determine the next steps. Minor issues can be covered with errata. For more significant updates, the corresponding Area Directors may charter a new working group to address the issues or individually sponsor an update.

- *For working group Internet-Drafts (files named draft-ietf-XXX-YYY)*, these are documents adopted for consideration by an IETF working group but are not yet finalized. The issue should be raised on the associated working group mailing list. The associated working group will work to vet the issue with you and come to a consensus on how to resolve the issue after notification. (see activity #9 of Figure 1)

- *For individual Internet-Draft submissions (files named draft-ZZZ-AAA)*, these are not officially adopted documents in the IETF. Such documents were submitted for consideration by the IETF for adoption by their author(s). Any issues found should be discussed with the authors (see Activity #7 of Figure 1). Despite not being formally adopted, a working group may be tracking or discussing such documents. Therefore, discussion of the issue may be appropriate on the working group mailing list. Note that there are rare instances where a document with this naming convention is adopted by a working group or is being advanced to publication as an RFC without being submitted to a working group (i.e., individual submission).

Vulnerabilities found in working group Internet-Drafts or individual submission documents that have expired, or were fixed in subsequent versions; or published RFCs that are marked historic, are unlikely to have action taken on them.

Generally speaking, being available for follow-up clarifications and related discussions posed by the Area Directors, Working Group Chairs, working group participants, or document authors is extremely helpful.

The IETF does not pay “bug bounties” for reported vulnerabilities.

Reporting a Vulnerability

The IETF produces documents in a distributed, organizational fashion. Working groups are chartered to define these documents. After the work is completed, they are closed. Therefore, there is not a single routing mechanism in the IETF to handle reported vulnerabilities. Depending on the maturity and circumstances of a given document, the reporting paths vary. No vulnerability is the same, but consult Figure 1 to understand how to report the vulnerability. Each activity in Figure 1 is documented below.

If this isn’t appropriate for your situation, or as a last resort, a vulnerability report can be sent to the <protocol-vulnerability@ietf.org> and the Security Area Directors will make a best effort to triage and action the information. This email alias does not have a public archive. If explicitly requested by the vulnerability reporter, information about the reporter can be removed when the Area Directors forward along the vulnerability information to public mailing list(s) (as noted above in the “Transparency in the IETF” and Activity #10 of Figure 1).

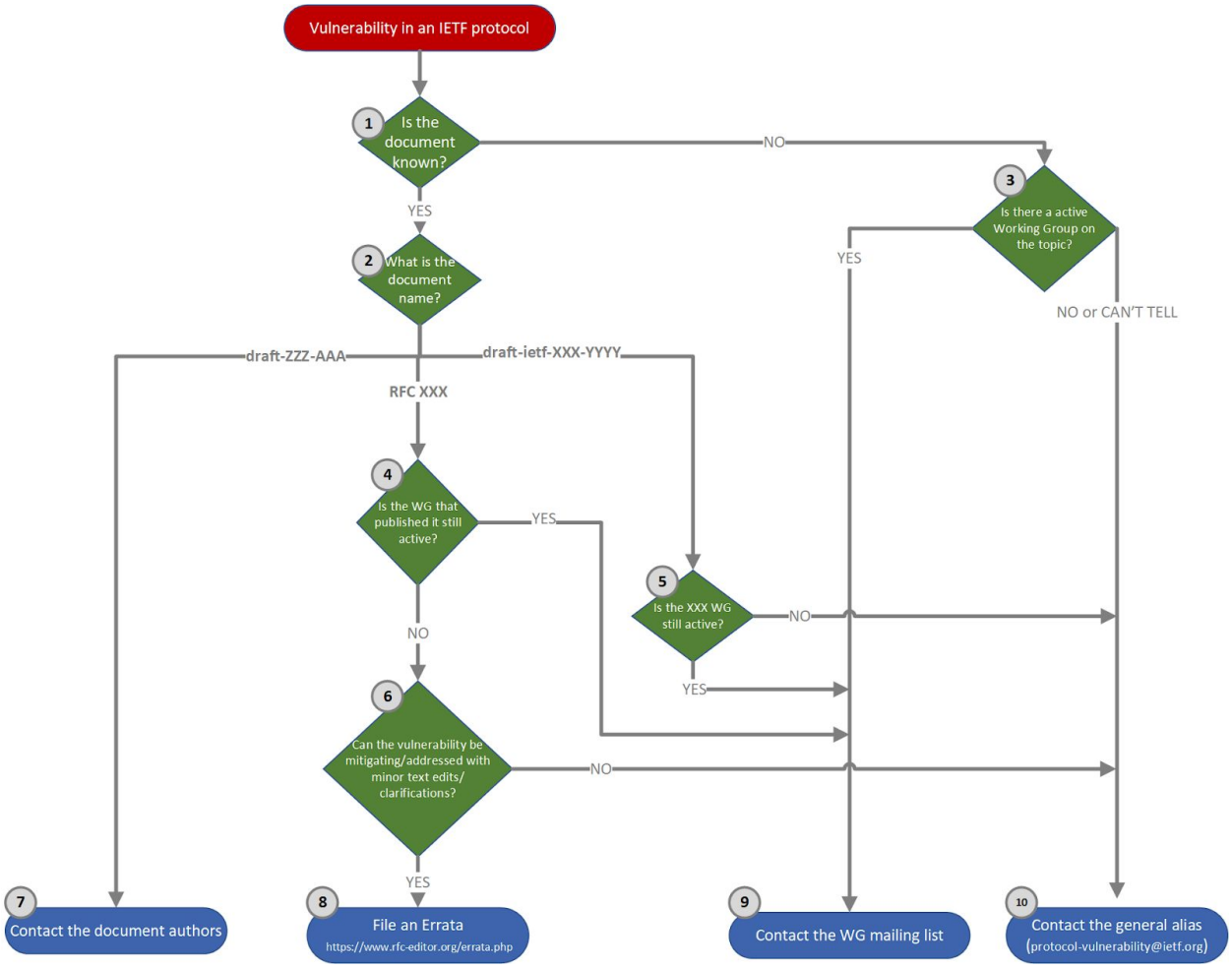

Figure 1: Vulnerability Reporting Flow

1. Is the document known?

Can the specific document in which the vulnerability is present be identified? All IETF documents are published in the [IETF Datatracker](https://datatracker.ietf.org)..

2. What is the document name?

What is the name of the document in which the vulnerability is present? Published documents have the naming convention of RFCxxxx (where xxxx is a four digit number). Internet-Drafts adopted by a working group have a naming convention of draft-ietf-xxx-yyy (where xxx is the working group in which the work is being done; and yyy is the chosen filename). Individual submissions, drafts that are not adopted

by a working group are named draft-ZZZ-AAA (where ZZZ-AAA are dictated by the document authors).

See Section 7 of https://www.ietf.org/standards/ids/guidelines/#7 for additional background on naming of IETF documents.

3. Is there an active working group on the topic?

Consult the list of active working groups.

4. Is the working group that published the document still active?

To determine if a working group that produced a document named XXX is active:

- Goto https://datatracker.ietf.org/doc/XXX/
- Click the “Status” tab
- In the “Document” meta-data section, find the “Type” field. Assuming it is a working group document, this field should have the value of either “Expired Internet-Draft (YYY WG)” or “Active Internet-Draft (YYY WG)”
- Clicking on the “YYY WG” link will bring up the associated working group page.

If the originating working group is found not to be active, also review the list of active working groups per Activity #3. A number of protocol maintenance work groups (e.g., LAMPS to address the maintenance of PKI specifications; TCPM to address TCP maintenance) have been established to update older, widely used protocols.

5. Is the “YYY” WG still active?

The procedure is the same as for Activity #4.

6. Can the vulnerability be mitigated/addressed with minor text edits or clarifications?

Judging “minor text edits or clarifications” is subjective. Generally speaking a “minor” edit meets the definition of an errata that is meant ‘to fix "bugs" in the specification and should not be used to change what the community meant when it approved the RFC.’

7. Contact the document authors

The contact information for all authors can be found at the end of each document.

8. File an Errata

An errata for published RFCs can be filed at https://www.rfc-editor.org/errata.php.

9. Contact the WG mailing list

Send your vulnerability report to the appropriate, public WG mailing list. To determine the mailing list of a working group named YYY identified in Activity #3 or 4.

- Goto https://datatracker.ietf.org/wg/YYY/about/
- Find the mailing list information in the section named “Mailing list”

Note that the mailing list name might not be the same as the working name.

For anything sent to a WG list, also consider sending a CC: to the general reporting alias, <protocol-vulnerability@ietf.org>, to provide additional visibility to the Security Area Directors.

10. Contact the general alias

As a last resort, vulnerability reports can always be sent to the <protocol-vulnerability@ietf.org> and the Security Area Directors will make a best effort to triage and action the information.