RSSAC Caucus Statement of Work for RSS Security Incident Reporting

May 16 2023

Background

RSSAC058 states that "The [eventual] RSS governance structure must include provision for cyber incident oversight and disclosure obligations, and codify security threat and vulnerability information sharing amongst RSOs and the [eventual governance structure]."[1] At ICANN74 the RSSAC decided to charter an RSSAC Caucus work party to provide advice on this topic. This document provides a statement of the work.

Goals of the Work

1. Focus on the RSS, as a system, versus RSOs individually to the extent possible.
2. In light of the governance structure evolution, propose new processes by parties to call for incident reporting and response, consider whether the new governance structure should be a *facilitator* for inter-RSO security incident handling, and/or be a clearing house for security incident reports.
3. Acknowledge relevant history of security events (e.g., DDOS attacks on 2016/06/25[2]) and document what the group of RSOs is currently doing. This could serve as a template for future reporting mechanisms.
4. Make recommendations to the RSS GS on the structure and scope of security incident disclosure for the Root Server System.
5. Maintain/improve confidence in the RSS by providing incident reporting.
6. Consider reasonable concerns from governments or other stakeholders about incident reporting.

Recognizing a certain level of subjectivity, the work party should focus on security incidents that have a *material adverse effect* on the root service. The following are out of scope for this work party:

- Incidents that affect RSOs without affecting their root server operations.
- Evaluation of individual RSOs or determining which RSOs are better or worse at responding to incidents. RSO independence as documented in RSSAC042 will remain an important consideration during the course of this work party.[3]

[1] See RSSAC058: Success Criteria for the RSS Governance Structure

[2] See https://root-servers.org/media/news/events-of-20160625.txt

[3] See RSSAC042: RSSAC Statement on Root Server Operator Independence

The eventual publication will need to be flexible enough to take into account changes in technology, yet proscriptive enough to distinguish between incidents that require a report and incidents that do not.

The primary audience of this publication will be the RSS Governance Structure (GS) and the primary purpose will be to assist the GS to implement the aforementioned criterion from RSSAC058. Additional audiences may include governments and other RSS stakeholders.

Scope

The WP will answer the following questions regarding incident reporting.

1. **Why should the RSS provide incident reporting?**
   a. Maintain/improve confidence in the RSS
   b. Consider reasonable concerns from governments or other stakeholders about incident reporting.

2. **What consists of a reportable incident? – Keep this at a high-level only**
   a. Boundaries of incidents versus non-incidents
      i. Attacks are not necessarily incidents, as they happen all the time.
      ii. Threshold to qualify an incident is subjective (e.g., DoS bps rates).
      iii. "Material effect"
   b. Categories of incidents and what is in scope of the RSS and what is not
      i. Incidents affecting availability
      ii. Incidents affecting data integrity
      iii. Incidents affecting confidentiality/privacy

3. **Who should be responsible for reporting incidents?**
   a. Who has authority to decide whether or not a particular incident warrants reporting?
   b. What should the governance body do to preserve the high level and quality of RSO collaboration regarding security incidents?
      i. Should RSS GS be a facilitator for inter-RSO security incident handling?
      ii. Should RSS GS be a facilitator to be a clearing house for security incident reports?
      iii. Should RSS GS be the provider of emergency communication channels?
   c. What are the roles of the RSS GS and RSOs with respect to reporting?
4. **How would incident reporting work?**
   a. How soon after an incident must a report be generated?

b. Should there be different levels of publication?
  i. Discussion/Publications among RSOs for lessons learned
  ii. Publications to the general public for transparency of the RSS.

c. What mandatory content should be in the report?
  i. Event timeline, root cause, actions taken, etc.

d. Is there a distinction between publicly reported incidents and non-publicly reported incidents?

Deliverable & Timeline

A ***final draft*** to be voted upon by the RSSAC before becoming an RSSAC publication.

Date of Delivery

The final draft should be submitted to the RSSAC no later than February 1st, 2025. Submission prior to the deadline is welcome.

- By ICANN 77, statement of work.
- By ICANN 81, first draft published for comment
- By ICANN 82, the work is approved by RSSAC.

Guidelines

This effort is to be carried out on the main RSSAC Caucus mailing list and involve any member of the RSSAC Caucus that wishes to participate. $WP_LEADER has agreed to be the champion for this work. They will ensure the work progresses forward and give updates on the work effort at RSSAC Caucus meetings and monthly RSSAC meetings. In the event that the deadline will not be realized, the champion should inform RSSAC and provide details of the work that cannot be completed by the deadline.

RSSAC support staff will assist the work party deliberation of the work, including setting up a mailing list for the work party, arranging and supporting regular teleconference calls, taking notes of meetings, and drafting background materials if needed.

References

Background Paper on RSS Cyber Incident Oversight and Disclosure Obligations
https://docs.google.com/document/d/1sCAbEk9hj_LShUSdU-iGBWrcxU7Txj8fRAXtX1X_5UQ/

RSSAC042: RSSAC Statement on Root Server Operator Independence
https://www.icann.org/en/system/files/files/rssac-042-17may19-en.pdf

RSSAC058: Success Criteria for the RSS Governance Structure
https://www.icann.org/en/system/files/files/rssac-058-17nov21-en.pdf