Trail of Bits Citation Guidelines

These guidelines explain how our clients may use Trail of Bits assessment reports in their sales, marketing, and/or promotional materials.

Introduction

Trail of Bits has created these guidelines to help parties understand how their company can use the results of a Trail of Bits security review in a fair and objective fashion to communicate the strengths of their service or product.

Trail of Bits strives to create guidelines that uphold a mutually respectful environment that is fair to all parties and reinforce Trail of Bits' value as an objective and independent security provider.

Trail of Bits Security Review Methodology Overview

Our evaluations allow our clients to make informed decisions about risk to their systems, and what security-relevant modifications may be necessary for a secure deployment.

Using our custom tools and unique expertise with static analysis, fuzzing, and concolic testing, we serve as a knowledgeable, dedicated adversary to identify the vulnerabilities that otherwise go undetected.

Our assessments provide an estimate of overall security posture, and the difficulty of compromise from an external attacker. We identify design-level risks and implementation flaws that illustrate systemic risks. At the conclusion of every assessment, we provide recommendations on best practices that could improve resistance to attack, and educate in-house security teams on common and novel security flaws and testing techniques.

At the end of every assessment, Trail of Bits provides a final report with an analysis of the system's overall security risk based on the findings. We encourage our clients to publicly share assessment results and often aid in reviewing blog posts or whitepapers for publication. In attempts to protect the message that is delivered with the Trail of Bits name attached to it, we have developed guidelines for citing the company in published work.

Note: These guidelines do not override any obligations under the MSA or constitute our consent to disclosure of TOB confidential information or use of TOB's name or trademarks.

Steps to publish Trail of Bits Work Product

1. Client informs Trail of Bits of their intention to publish the audit report
    a. Client provides Trail of Bits with an opportunity to review/suggest messaging in prewritten:
        i. Blog posts.
        ii. Tweets.
        iii. Press releases.
    b. Trail of Bits copy-edits the report and finalizes it for publication.
2. Trail of Bits publishes the report the same day as Client's announcement on Trail of Bits' GitHub Publications page:
    a. Including the name of the product, a link to the report, the approximate month of the work, and the amount of time we spent on the review
3. Client includes a link in announcement to the published report on Trail of Bits' GitHub Publications page.

Guidelines

Follow these guidelines for publishing Trail of Bits final reports and announcing having worked with Trail of Bits:

1. Clients must not make any announcements, publications, or otherwise describe our work unless they coordinate with us to get the language approved.
2. Clients should not announce an intention to work with Trail of Bits as this may imply Trail of Bits' endorsement of clients' products and their security before an assessment is complete.
3. Clients must not refer to Trail of Bits as a "Partner." Trail of Bits is solely contracting with clients as a vendor.
4. Trail of Bits will not provide comments or quotes surrounding audit results or overall security of product outside of the delivered report.
    a. Trail of Bits can suggest information to highlight in releases and assist with reviewing material ahead of public dissemination.
5. Clients may cite Trail of Bits' work product when following the guidelines below:
    a. Citation must be verbatim from the final deliverable. It cannot be summarized, modified, or manipulated in any way.
    b. Citing Trail of Bits to say, "PRODUCT_NAME is secure because an audit was completed by Trail of Bits" is not sufficient.

Other Usage Guidelines

- Clients may use the Trail of Bits logo in blog posts, white papers, and press releases as long as the graphic is shown in its entirety and unaltered.
- Clients may use the Trail of Bits logo in presentations to live audiences as long as the graphic is shown in its entirety and unaltered.

Trail of Bits' logo is available via https://www.trailofbits.com/assets/files/presskit.zip

Appendix: Example Citations

You can find examples of clients mentioning Trail of Bits in their publications on our GitHub Publications page.

Proper examples of mentioning and citing Trail of Bits

> "Our Product's GitHub repository includes documentation, a comprehensive test suite, and an independent third-party audit by the security research firm Trail of Bits."
>
> "We also have a new audit available, thanks to the Trail of Bits team. We engaged Trail of Bits to undertake an audit of all three libraries mentioned above, with the RZL MPC paper and MPC wiki as documentation/guidelines for expected behaviour. In evaluating the code maturity (quoting directly from the audit):
>
> - Arithmetic: 'Moderate. We reported various findings related to arithmetic. However, these largely represent improvements and are not currently exploitable issues.'"
>
> "Sweet B is designed to provide a new level of safety and assurance in open source elliptic curve cryptography and its GitHub repository includes documentation, a comprehensive test suite, and an independent third-party audit by the security research firm Trail of Bits."
>
> "We are proud to announce that the etcd team has successfully completed a 3rd party security audit for the etcd latest major release 3.4. The third party security audit was done for etcd v3.4.3 by Trail of Bits. A report from the security audit is available in the etcd community repo."
>
> "Trail of Bits performed a private red team exercise on the system and identified a number of risks that have been fixed for 20.07:
>
> - The /proc file system on Linux is mounted rw giving the ability to write to /proc/self/mem allowing unsigned code execution, /proc/self/mem is now read-only
> - The internal GetRandom() function failed to properly fill in buffers that have a length that is not a multiple of 4, all current usage is a multiple of 4 so no risk and code was changed to avoid future impacts...."

Improper examples of mentioning and citing Trail of Bits

“The Client team was quick to address all of the recommendations provided by Trail of Bits in the final report. TOB was impressed by the team's expertise and prioritization of security."
—Goes against:

- Guideline 5.a.: “Citation must be verbatim from the final deliverable. It cannot be summarized, modified, or manipulated in any way.”
- Guideline 4: “Trail of Bits will not provide comments or quotes surrounding audit results or overall security of product outside of the delivered report.”

“We have partnered with Trail of Bits for an upcoming security review of our new product, stay tuned for the results!”
—Goes against:

- Guideline 2: “Clients should not announce an intention to work with Trail of Bits.”
- Guideline 3: “Clients must not refer to Trail of Bits as a ‘Partner.’”

“XZJ Protocol will be audited and the technology is open source. We are glad to announce that the first iteration of the protocol will be audited by Trail of Bits, who is a world leader in the information security industry, particularly around bytecode analysis of compiled software.”
—Goes against:

- Guideline 2: “Clients should not announce an intention to work with Trail of Bits.”