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 risks 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 vulnerabilities that otherwise go undetected.

Our assessments estimate the 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 to improve resistance to attacks 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 analyzing the system's overall security risk based on the findings. We encourage our clients to publicly share assessment results and often assist in reviewing blog posts or whitepapers for publication. We have developed guidelines for citing the company in published work to protect the message delivered with the Trail of Bits name attached to it.

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

ⓒ 2024 Trail of Bits

Steps to Publish Trail of Bits Work Product

- The client informs Trail of Bits of their intention to publish the audit report.
  If you choose to publicize a previously confidential report, please reach out to Trail of Bits.
- Client provides Trail of Bits with an opportunity to review/suggest messaging in prewritten:
    - Blog posts.
    - Social Media Posts
    - Press releases.
    - Quotes or comments given to the press
- Trail of Bits copy-edits the report and finalizes it for publication.
- Trail of Bits publishes the report the same day as the Client's announcement on Trail of Bits' GitHub Publications page:
    - 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.
- The client includes a link to the published report on Trail of Bits' GitHub Publications page in the announcement.

Social Media Guidelines

When citing Trail of Bits on social media after approval, please tag Trail of Bits using the following social media accounts.

- X: @TrailofBits
- X: @TrailofBlocks **If Trail of Bits agrees to retweet a client's post that is blockchain-related, this handle will be used **
- LinkedIn:https://www.linkedin.com/company/trail-of-bits
- Mastodon: https://mastodon.social/@trailofbits@infosec.exchange
- Warpcast:@trail-of-blocks

Guidelines

Follow these guidelines for publishing Trail of Bits 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 approve the language. Furthermore, clients must gain approval to tag Trail of Bits social media handles.
2. Clients should not announce their intention to work with Trail of Bits before an assessment is complete, as this may imply Trail of Bits' endorsement of clients' products and their security.
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 regarding audit results or the overall security of a product outside of the delivered report material.
    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,
6. Clients must avoid using absolute phrases like "we are working with Trail of Bits to confirm our security" or "Our company passed the Trail of Bits audit". At Trail of Bits our assessments are not check boxes or graded reports but assessments with recommendations for improvements.
7. Clients must not use phrases that can be interpreted as your project or product is completely secure now that a Trail of Bits audit is complete
8. Clients must refrain from using the name "Trail of Bits" in assertive phrases that imply endorsement.
9. Clients must avoid using language that implies comprehensive security based solely on the audit. Instead, they should accurately specify the scope of the assessment, acknowledging that the audit covers only specific aspects or components of their product or system. This ensures a precise representation of the audit's findings and avoids giving a false impression of complete security.
10. The full name of Trail of Bits must be used in citations; shortening the name to TB, Trail of B, or any other variation is prohibited

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 behavior. ’”

“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 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….”

Improper Examples of Mentioning and Citing Trail of Bits

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

—Goes against:

Guideline 3: “Clients must not refer to Trail of Bits as a ‘Partner.’”

"Trail of Bits confirmed that our smart contracts are secure"

—Goes against:

- Guideline 6: “Clients must avoid using absolute phrases”
- Guideline 7: “Clients must not use phrases that can be interpreted as your project or product is completely secure now that a Trail of Bits audit is complete”

“We passed a Trail of Bits audit”

—Goes against:

- Guideline 6: “Clients must avoid using absolute phrases”

Steps Taken for Not Following Our Guidelines

Trail of Bits requires explicit permission for the use of our name, logo, social media handles, and any of our work in public domains. If a client, partner, or any third party uses these assets without prior authorization, we will take the following actions:

1. Immediate Request for Compliance: Trail of Bits will promptly reach out to the involved party to request edits or removal of the unauthorized content.
2. Enforcement Measures: If the requested action is not taken in a timely manner, Trail of Bits will proceed to file a Digital Millennium Copyright Act (DMCA) violation against the offending party.

These steps ensure that our brand integrity and intellectual property rights are protected, maintaining the accuracy and integrity of information associated with Trail of Bits.

Co-Marketing

Engagement Policy:

- Trail of Bits engages in co-marketing activities selectively, based on the specifics of each case. Past activities have included co-branded social media posts, blogs, case studies, and live streams.

Steps for Co-Marketing:

- **Step 1**: Contact your Trail of Bits Project Manager to discuss the co-marketing opportunity.
- **Step 2**: If the project is deemed suitable, you will be connected with our Marketing Manager for further steps.

Types of Co-Marketing:

We have successfully partnered on various co-marketing initiatives, such as:

- **Social Media Posts**: Jointly branded posts to promote collaborative efforts.
- **Blogs**: Co-authored articles or guest posts highlighting mutual work.
- **Case Studies**: In-depth analysis and documentation of joint projects.
- **Live Streams**: Real-time, co-hosted events discussing industry topics or showcasing collaborative projects.

Review and Approval:

- Any co-marketing content must be reviewed and approved by Trail of Bits before publication to ensure alignment with our brand guidelines and messaging.

Flexibility and Adaptability:

- Each co-marketing initiative is tailored to fit the unique requirements of the collaboration, ensuring that both parties benefit and the integrity of the Trail of Bits brand is maintained.

Brand Guidelines

https://www.trailofbits.com/documents/210417_TrailOfBits_StyleGuide.pdf

Do not use the Trail of Bits Brand Assets as part of any of your own trademarks, logos, company names, icons, product or feature names, domain names, social media handles, or avatars. For example, do not physically combine or intermingle any Trail of Bits Brand Assets with your own trademarks or logo; they must remain separate.

Do not modify the Trail of Bits Brand Assets in any way, including by changing any colors or dimensions, obstructing or printing over any part of the asset, or adding your own design elements.

When you are designing your own website and marketing materials, do not imitate the distinctive look and feel of any of Trail of Bit's website, apps, logos, trade dress, slogans, taglines, color scheme, icons, or marketing materials. Also, do not register or use a domain name that incorporates "Trail of Bits" or any confusingly similar term in the domain name itself.

Do not use any Trail of Bits Brand Asset in a damaging or derogatory way, or in connection with any social media or website that violates any law.

You must obtain explicit permission from Trail of Bits before using our logo on any social media platforms, websites, blogs, press releases, or other forms of media.