Trail of Bits Citation Guidelines

Executive Summary

These guidelines explain how participating companies 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 developing 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.

Guidelines

After Trail of Bits has delivered a project's final deliverable, companies often issue their own press releases and other materials about the results. Clients can mention Trail of Bits in various ways, but when **citing** Trail of Bits, we suggest the following guidelines:

1. Citation must be verbatim from the final deliverable. It cannot be summarized, modified, or manipulated in any way.
2. Citing Trail of Bits to say, "PRODUCT_NAME is secure because an audit was completed by Trail of Bits" is not sufficient.
3. Trail of Bits will not provide comments or quotes surrounding audit results or overall security of product outside of the delivered report.

Some proper examples of mentioning and citing Trail of Bits can be found below:

> "Trail of Bits recommends contract migration instead of contract upgrades because upgradeability increases code complexity."
>
> "The auditor Trail of Bits completed the security review in October. In addition to publishing this report, we want to highlight several lessons we found especially valuable."
>
> "Trail of Bits's engineers, who bring deep backgrounds in security and Java, discovered some obscure vulnerabilities and bugs. For example, 'The `entrySet()` method of `java.util.map` is allowed to successively return a single, mutable `Entry` object instance, overwriting the object's contents during each iteration. Therefore, the `HashSet` created on line 63 of [the code] (cf. Figure 1.1) can potentially contain multiple copies of the same `Entry` object with contents equal to the last entry returned from `hashValueStore.entrySet()`.'"

NOTE: Trail of Bits can suggest information to highlight in releases and assist with reviewing material ahead of public dissemination.

Other Usage Guidelines

- 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.
- 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.

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

We recommend that customers write a blog post about working with us **only after the engagement has concluded** as the results may be critical or take months to fix. However, if a client must publicly announce an intent to work with Trail of Bits, then we require an executed Master Services Agreement and Statement of Work prior to publication. Below is an example of how to publicize upcoming work with Trail of Bits:

> "Security firm Trail of Bits has been hired to provide security auditing expertise as part of the cooperation. The Open Source Technology Improvement Fund (OSTIF) connected developers with multiple security teams and is coordinating audits of RandomX."
>
> "DLP 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."

Supplemental Material

Online Resources

You can find examples of past client's mention of Trail of Bits in their publications on our GitHub Publications page.

Steps to publish Trail of Bits security reviews

1. Customer informs Trail of Bits of their intention to publish the audit report
    a. Trail of Bits offers to review/suggest messaging in prewritten:
        i. Blog posts
        ii. Tweets
        iii. Press releases
2. Trail of Bits gives the report one more pass through copy editing, and delivers a final version to Customer prior to Customer's announcement
3. Trail of Bits publishes the report the same day as Customer's announcement
4. Customer includes a link in announcement to the published report on Trail of Bits' GitHub Publications page