

Vulnerabilities in WebAssembly: A Survey

Holger Klein
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany



Figure 1: Seattle Mariners at Spring Training, 2010.

ABSTRACT

A clear and well-documented \LaTeX document is presented as an article formatted for publication by ACM in a conference proceedings or journal publication. Based on the “acmart” document class, this article presents and explains many of the common variations, as well as many of the formatting elements an author may use in the preparation of the documentation of their work.

KEYWORDS

binary exploits, Webassembly, IT Security

ACM Reference Format:

Holger Klein. 2021. Vulnerabilities in WebAssembly: A Survey. In *Proceedings of ACM Conference (Conference’17)*. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 INTRODUCTION

Introduce the papers structure: State of the art What is wasm relevant features for vulnerabilities What are binary exploitation techniques usually used

Which can and cannot be used in wasm (picture/table?) Talk about wasabi Talk about own experiments?

[1]

2 WEBASSEMBLY

The following will give an Introduction to and an overview of Webassembly, paying special attention to the parts relevant to a

discussion of binary vulnerabilities. For more information, see the official specification at [2].

2.0.1 High Level Overview. The name Webassembly is a slight misnomer, since it is a different form and function than typical assembly languages. It is a binary byte code format which is interpreted by a virtual machine, most often a browser. It is supposed to run at near-native speeds. There exists a human-readable form of WebAssembly binaries called ‘wat’.

REFERENCES

- [1] Daniel Lehmann, Johannes Kinder, and Michael Pradel. 2020. Everything Old is New Again: Binary Security of WebAssembly. *Proceedings of the 29th USENIX Security Symposium* (Aug. 2020), 217–234.
- [2] Andreas Rossberg. 2021. *WebAssembly Specification*. <https://webassembly.github.io/spec/core/>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Conference’17, July 2017, Washington, DC, USA

© 2021 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>