liblzma - OSS and Backdoors

Exploring the xz-utils Backdoor, its Emergence and its Impact on FOSS and OSS

9525469

June 4, 2024

Abstract

In recent years, several vulnerabilities in the open-source software supply chain were discovered. The most recent being the intentionally placed backdoor in the compression library named *liblzma*. This paper aims to explore the implementation of said backdoor while highlighting the insertion of the backdoor and the inserters use of social engineering enabling their placement in the leadership of the project. Furthermore ways of preventing similar attacks are presented and evaluated on the example of the *liblzma* situation.

1 Introduction

FOSS[1] is generally defined as software the user can "[...] run, copy, distribute, study, change and improve [...]" [2]. This requires the source to be available and enables the dependence of other software on subsets or the entirety of the code. On the other hand, source available or OSS[2] are distinct from FOSS software. Some licenses do not require the resulting product to be licensed under the same license as its dependencies, such as the MIT license[3]. It therefore differs from the GPL[4] and software licensed with the MIT-Licence can therefore not be referred to as free open-source software, but rather as open-source software.

[1] Free and Open-Source Software [1]

[2] Open-Source Software

[3] Requires the license to be present in "all copies or substantial portions of the Software" [3]

[4] Requires all copies of the software to be licensed as GPL [4]

References

[1] R. M. S. (RMS). (2021), [Online]. Available: https://www.gnu.org/philosophy/pragmatic.html (visited on 06/04/2024).

[2] F. S. Foundation. (2024), [Online]. Available: https://www.gnu.org/philosophy/free-sw.html (visited on 06/04/2024).

[3] Opensource.org. (2024), [Online]. Available: https://opensource.org/license/MIT (visited on 06/04/2024).

[4] Opensource.org. (2024), [Online]. Available: https://opensource.org/license/gpl (visited on 06/04/2024).

Appendix