Follina and Confluence - ZeroDays Exploited

Jude Safo, S.M.,[1]★ Tahsin Saffat, Ph.D,[2] Riaz Bacchus[2,3] [3] Rafael Okure
[1]*Haiphen Inc., Bronx , NY 10454, USA*
[2]*California Institute of Technology - Department of Mathematics, 1200 E California Blvd, Pasadena CA 91125, USA*
[3]*Techstars, Seattle, Campus Box 354625, 1100 NE Campus Pkwy 200, Seattle, WA 98105*

13 June 2022

ABSTRACT
"87% of enterprise supply chain breaches involved software not directly present in their stack" - NIST Survey, 2021. Hence the motivation of this paper is to investigate the root cause of such incidents. June 6th, 2022, 1-week removed from the Microsoft 'Follina' exploit, CVE-2022-30190, and Confluence exploit, CVE-2022-26134, we identify the full *software dependency-chain* for each. We go one step further to identify the 'upstream' effects of these attacks (e.g. enterprises that consume the affected products) with an outlook on how to improve remediation efforts.

Key words: software supply chain – application security — zero-day attacks

1 INTRODUCTION

Cybersecurity only affects big companies like Reddit, Amazon and Apple, right? The 2021 colonial pipeline ransomware attack lead to a 10% increase the price of gas nationally. The price of beef increased 3% after the JBS ransomware attack. DDOS attacks have even been levied against pace-makers and NEST thermostats in the dead of winter. The world is more inter-connected than it has ever been and much of the industry is only realizing that now.

Threat actors employ different techniques to execute software supply chain attacks. Three common techniques are:

- Hijacking updates
- Undermining code signing
- Compromising open-source code

These techniques are not mutually exclusive, and threat actors often leverage them simultaneously.

2 UPSTREAM IMPACT

CVE-2022-30190 aka Follina:
The Microsoft Support Diagnostic Tool (MSDT) is quite serious with a CVSS score of 7.8. Hackers gain remote-code execution. Here's just a few ways hackers can and already have taken advantage of this. Confluence is present in over a dozen cloud providers

CVE-2022-26134 aka conlfuence
Among the upstream products consuming ... Co-dependence on Apache ... apache-archiva, apache-arrow, apache-ctakes, apache-drill, apache-flink, apache-forrest, apache-geode, apache-opennlp, apache-pulsar, apache-spark, ccache

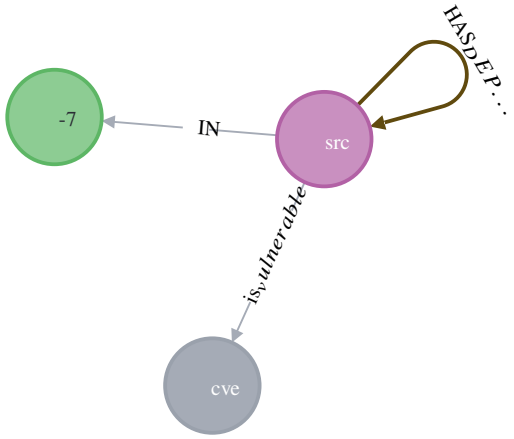

Figure 1. software dependency graph schema

3 DOWNSTREAM IMPACT

Organizations are uniquely vulnerable to software supply chain attacks for two major reasons: first, many third-party software products require privileged access; and second, many third-party software products require frequent communication between a vendor's network and the vendor's software product located on customer networks. **?**, and describes the problem the authors aim to solve (e.g. Van Dijk 1902). Multiple citations can be joined in a simple way like De Laguarde (1903); De la Guarde (1904). Section 3.1 below.

3.1 Open Source Dependency Chain

Open-source code compromises occur when threat actors insert malicious code into publicly accessible code libraries, which unsuspecting developers—looking for free blocks of code to perform specific functions—then add into their own third-party code. For example, in 2018, researchers discovered 12 malicious Python libraries uploaded on the official Python Package Index (PyPI). The attacker used ty-

★ E-mail: pi@haiphenai.com (haiphen)

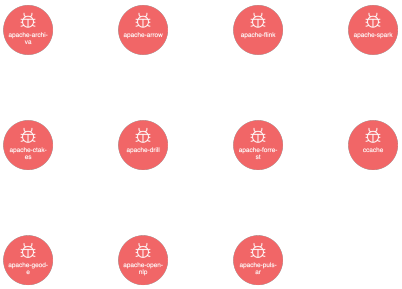

Figure 2. Infected apache software stack

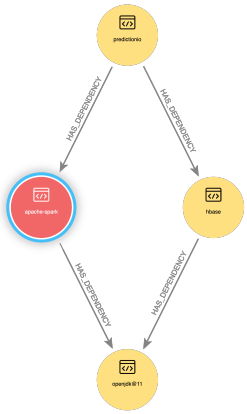

Figure 3. Software dependency chain

Table 1. Root node and it's software dependencies

apache-flink	apache-spark	apache-opennlp	apache-forrest
openjdk@11	predictionio	openjdk@11	openjdk@11
X	openjdk@11	X	X
X	hbase	X	X

posquatting tactics by creating libraries titled "diango," "djago," "dajngo," etc., to lure developers seeking the popular "django" Python library. The malicious libraries contained the same code and functionality of those they impersonated; but they also contained additional functionality, including the ability to obtain boot persistence and open a reverse shell on remote workstations.9 Open-source code compromises can also affect privately owned software because developers of proprietary code routinely leverage blocks of open-source code in their products. $2 \times 3 = 6$ or $v = 220\,\mathrm{km\,s^{-1}}$, but more complicated expressions should be entered as a numbered equation:

4 CONCLUSIONS

Certain simplifications were made for the sake of ... In reality the apache dependencies sit lower in the stack than confluence ... Doing a simple analysis of the open source dependency chain and ...

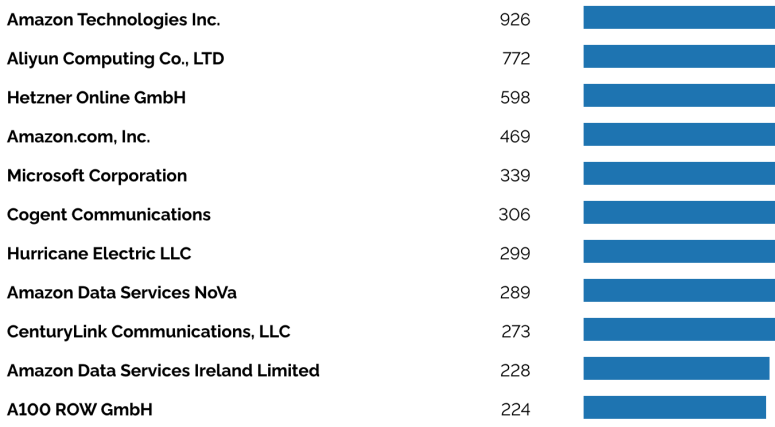

Figure 4. Affected Organizations

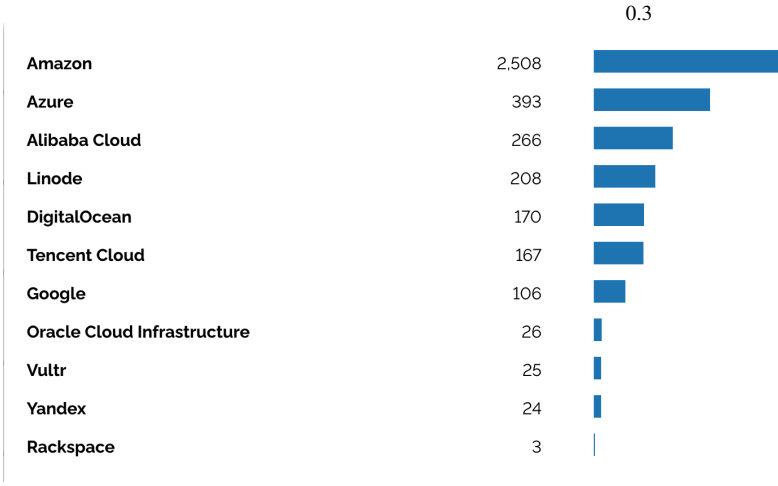

Figure 5. Affected Cloud Providers

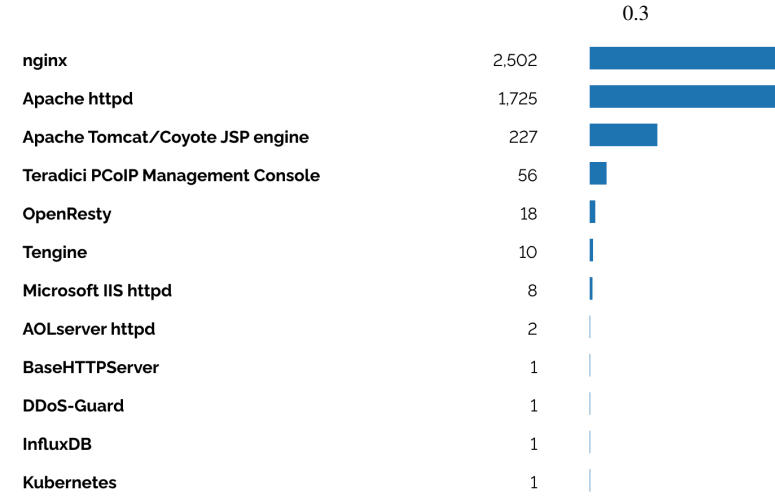

Figure 6. Affected Products

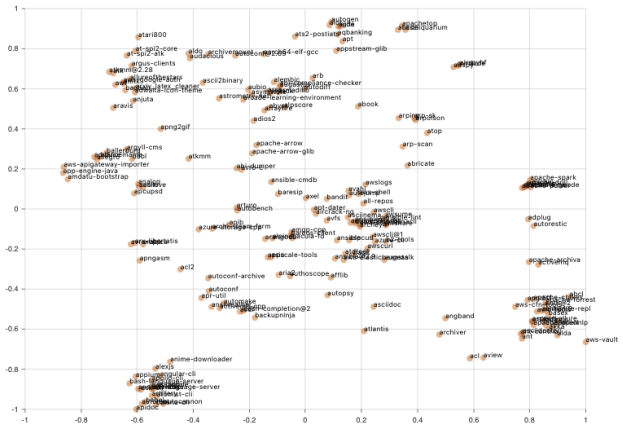

Figure 7. Principal component analysis of several software libraries

ACKNOWLEDGEMENTS

This work is supported by Techstars and Filecoin.

DATA AVAILABILITY

The inclusion of a Data Availability Statement is a requirement for articles published in XXXX. Data Availability Statements provide a standardised format for readers to understand the availability of data underlying the research results described in the article. The statement may refer to original data generated in the course of the study or to third-party data analysed in the article. The statement should describe and provide means of access, where possible, by linking to the data or providing the required accession numbers for the relevant databases or DOIs.

REFERENCES

van Dijk T., 1902, QJRAS, 2, 202
de la Guarde S., 1904, MNRAS, 4, 404
de Laguarde A., 1903, Nat, 3, 303

APPENDIX A: DEFINITIONS

OSS: Open Source Software CVE: Common Vulnerability Exploit

This paper has been typeset from a TEX/LATEX file prepared by the author.