EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate B - Digital Business Solutions
DIGIT B3 - Reusable Solutions

EU-FOSSA 2

WP5 D3.1 Bug Bounties Summary

TABLE OF CONTENTS

1. INTRODUCTION

EU-FOSSA 2 (EU Free and Open Source Software Auditing) was a Preparatory Action no. 26.03.77.06 run during 2017-2020. It was a continuation of the successful EU-FOSSA Pilot Project (26.03.77.02).

1.1. Purpose of the document

This document summarises the results from the bug bounties carried out by the project's bug bounty partners. It also includes in the appendices the closure reports from HackerOne and Intgriti/Deloitte.

2. Bug Bounties Selected

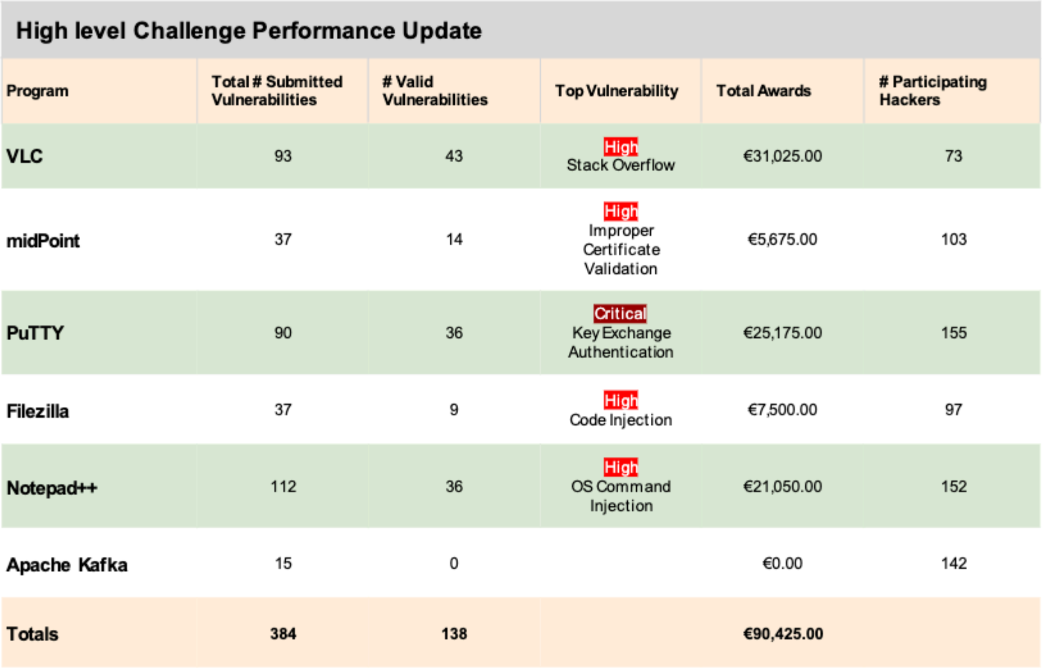
The EU-FOSSA 2 project selected 15 open source software for bug bounties. To see the rationale that led to this selection, please refer to deliverable D2.3 on the following page: https://joinup.ec.europa.eu/solution/eu-fossa-pilot/document/project-deliveries.

The table below shows the selected software and the company that carried out the bug bounty.

Bug bounty software	Platform Provider
1. Apache Kafka	Hacker One
2. FileZilla	Hacker One
3. Midpoint	Hacker One
4. Notepad++	Hacker One
5. PuTTY	Hacker One
6. VLC	Hacker One
7. 7-zip	Intigriti/Deloitte
8. Apache Tomcat	Intigriti/Deloitte
9. Drupal	Intigriti/Deloitte
10. DSS	Intigriti/Deloitte
11. Flux TL	Intigriti/Deloitte
12. Glibc	Intigriti/Deloitte
13. KeePass	Intigriti/Deloitte
14. PHP Symfony	Intigriti/Deloitte
15. WSO2	Intigriti/Deloitte

3. HackerOne Results

This section shows the results of the HackerOne allocated bug bounties.



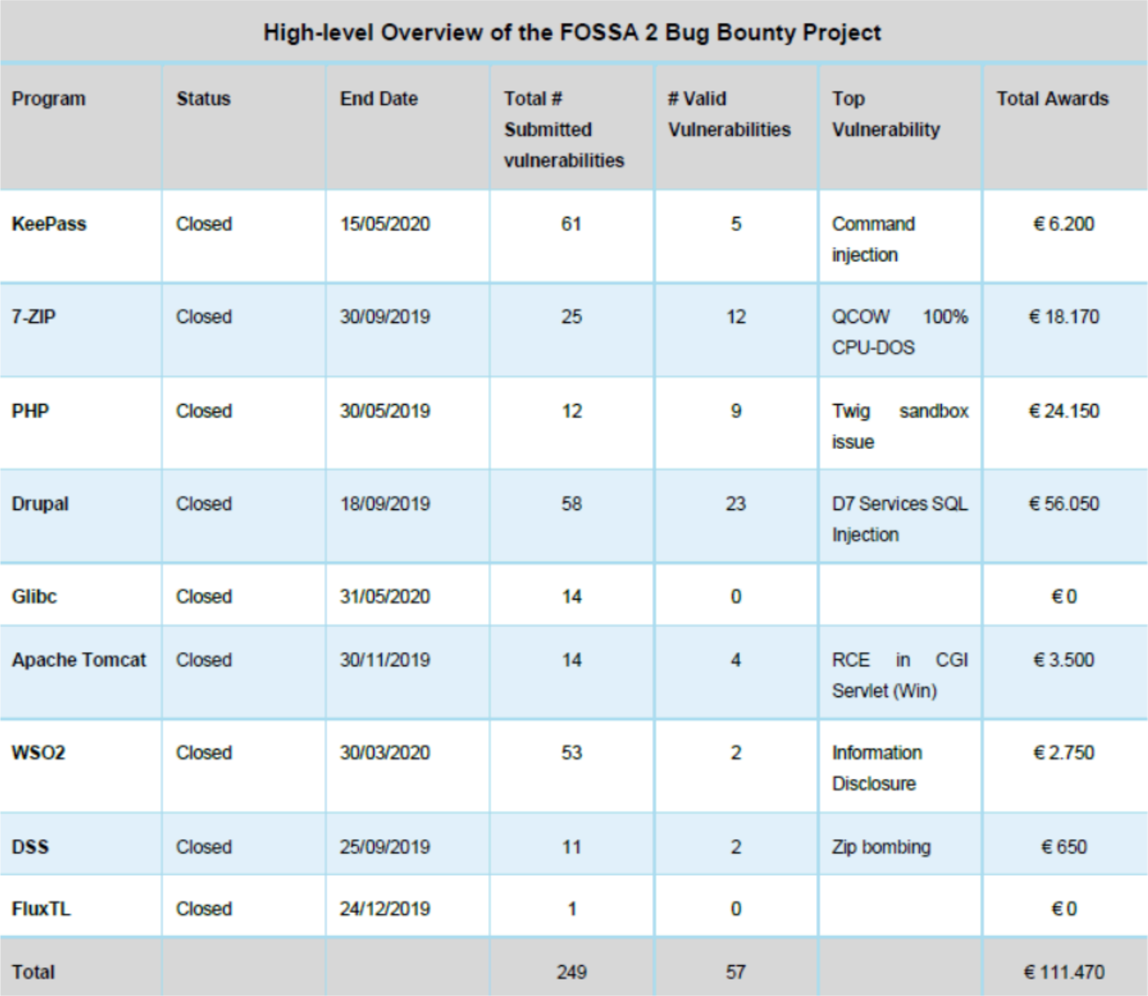
High level Challenge Performance Update

Program	Total # Submitted Vulnerabilities	# Valid Vulnerabilities	Top Vulnerability	Total Awards	# Participating Hackers
VLC	93	43	High Stack Overflow	€31,025.00	73
midPoint	37	14	High Improper Certificate Validation	€5,675.00	103
PuTTY	90	36	Critical Key Exchange Authentication	€25,175.00	155
Filezilla	37	9	High Code Injection	€7,500.00	97
Notepad++	112	36	High OS Command Injection	€21,050.00	152
Apache Kafka	15	0		€0.00	142
Totals	**384**	**138**		**€90,425.00**	

Severity	1. Critical		2. High		3. Medium		4. Low		Total	
Program	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards
Vlc_h1c	0	€ 0	2	€ 5.000	19	€ 20.250	21	€ 5.400	42	€ 30.650
Putty_h1c	1	€ 6.000	2	€ 6.500	5	€ 5.050	28	€ 7.300	36	€ 24.850
Notepad-plus-plus	0	€ 0	3	€ 8.150	5	€ 5.300	29	€ 7.400	37	€ 20.850
Midpoint_h1c	0	€ 0	1	€ 1.800	9	€ 4.900	4	€ 700	14	€ 7.400
Filezilla-h1c	0	€ 0	1	€ 3.250	0	€ 0	8	€ 2.400	9	€ 5.650
Apache_kafka_h1c	0	€ 0	0	€ 0	0	€ 0	0	€ 0	0	€0
Total	**1**	**€ 6.000**	**9**	**€ 22.900**	**38**	**€ 35.500**	**90**	**€ 23.200**	**138**	**€89.400**

4. Intigriti/Deloitte Results

Intigriti received 249 vulnerability submissions for the 9 bug bounties it was running. Of these, 57 submissions were accepted and payments made (22.8%) and 192 were rejected (77.1%). Out of the 192 rejections, 14 were duplicates. Taking duplicates into account 24.3% of submissions were accepted and 75.7% rejected.



High-level Overview of the FOSSA 2 Bug Bounty Project

Program	Status	End Date	Total # Submitted vulnerabilities	# Valid Vulnerabilities	Top Vulnerability	Total Awards
KeePass	Closed	15/05/2020	61	5	Command injection	€ 6.200
7-ZIP	Closed	30/09/2019	25	12	QCOW 100% CPU-DOS	€ 18.170
PHP	Closed	30/05/2019	12	9	Twig sandbox issue	€ 24.150
Drupal	Closed	18/09/2019	58	23	D7 Services SQL Injection	€ 56.050
Glibc	Closed	31/05/2020	14	0		€ 0
Apache Tomcat	Closed	30/11/2019	14	4	RCE in CGI Servlet (Win)	€ 3.500
WSO2	Closed	30/03/2020	53	2	Information Disclosure	€ 2.750
DSS	Closed	25/09/2019	11	2	Zip bombing	€ 650
FluxTL	Closed	24/12/2019	1	0		€ 0
Total			249	57		€ 111.470

Severity	1. Critical		2. High		3. Medium		4. Low		Total	
Program	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards
KeePass	0	€ 0	0	€ 0	1	€ 3.900	4	€ 2,300	5	€ 6,200
7-ZIP	0	€ 0	2	€ 10,000	4	€ 6.000	6	€ 2,170	12	€ 18,170
PHP	2	€ 17,000	2	€ 1,500	4	€ 5,300	1	€ 350	9	€ 24,150
Drupal	0	€ 0	8	€ 41,000	8	€ 12,600	7	€ 2,450	23	€ 56,050
Glibc	0	€ 0	0	€ 0	0	€ 0	0	€ 0	0	€ 0
Apache Tomcat	0	€ 0	1	€ 2,500	1	€ 500	2	€ 500	4	€ 2,500
WSO2	0	€ 0	1	€ 2,500	0	€ 0	1	€ 250	2	€ 2,750
DSS	0	€ 0	0	€ 0	1	€ 500	1	€ 150	2	€ 650
FLUX	0	€ 0	0	€ 0	0	€ 0	0	€ 0	0	€ 0
Total	2	€ 17,000	14	€ 57,500	19	€ 28.800	22	€ 8.470	57	€111,470

Appendix A: HackerOne Closure Report

Vulnerabilities All-Time		**Bounty** All-Time				**Hackers** All-Time	
384 #Submits	117 #Resolved	138 Count	€ 89.400 Total €	€ 6.000 Largest	176 Submitted	46 Resolved	€ 11.800 Top Paid
80 (crit/high)	9 (crit/high)	10 (crit/high)	30.6652 (crit/high)		60 (crit/high)	8 (crit/high)	0 (crit/high)
7.4 Median First Response (in bus hrs)		16.9 Median Hours to Triage (in bus hrs)		9.2 Median to Bounty (in bus hours)		30.9 Median to Resolve (in bus days)	
2.1 (crit/high)		4.9 (crit/high)		10.5 (crit/high)		19.0 (crit/high)	

Severity	**1. Critical**		**2. High**		**3. Medium**		**4. Low**		**Total**	
Program	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards	Count	Total Rewards
Vlc_h1c	0	€ 0	2	€ 5.000	19	€ 20.250	21	€ 5.400	42	€ 30.650
Putty_h1c	1	€ 6.000	2	€ 6.500	5	€ 5.050	28	€ 7.300	36	€ 24.850
Notepad-plus-plus	0	€ 0	3	€ 8.150	5	€ 5.300	29	€ 7.400	37	€ 20.850
Midpoint_h1c	0	€ 0	1	€ 1.800	9	€ 4.900	4	€ 700	14	€ 7.400
Filezilla-h1c	0	€ 0	1	€ 3.250	0	€ 0	8	€ 2.400	9	€ 5.650
Apache_kafka_h1c	0	€ 0	0	€ 0	0	€ 0	0	€ 0	0	€0
Total	**1**	**€ 6.000**	**9**	**€ 22.900**	**38**	**€ 35.500**	**90**	**€ 23.200**	**138**	**€89.400**

APPENDIX B: INTIGRITI/DELOITTE CLOSURE REPORT