EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate B - Digital Business Solutions
DIGIT B3 - Reusable Solutions

Brussels, 26 October 2018

EU-FOSSA 2

Bug Bounty Candidates and Rationale

1. BUG BOUNTY PROGRAMME

The EU-FOSSA 2 project is running bug bounties on identified open source software in order to find high quality security vulnerabilities (or bugs). The project is looking to run around fifteen to twenty bug bounties, and so ideally needs a target software list of thirty to select from.

This document describes the various stakeholders and their needs, the rationale for selecting software, the selection process, and the final list of software proposed.

2. STAKEHOLDERS AND THEIR NEEDS

The key stakeholders of the EU-FOSSA 2 project include the:

1. European Commission
2. Other participating European Institutions
3. EU Public
4. Open source software development communities
5. Open source Development Groups within the European Institutions

2.1. European Commission

The EU-FOSSA Pilot project conducted an exercise in 2016 to identify the open source software it was using within its various functions. The EU-FOSSA 2 project is refreshing this list over the next two months, and expanding it to include development tools and methods. Of the software identified, it makes sense for the Commission to consider the most critical, i.e.

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË — Tel. +32 22991111
Office: MO15 04/P034

Commission européenne, 2920 Luxembourg, LUXEMBOURG — Tel. +352 43011

those that could cause the maximum damage if they have any undiscovered security vulnerabilities. The 2016 inventory exercise identified 23 software as *critical*.

The table below has 22 entries, with nss & npr grouped together, there are 23 entries. The known omission from this list is *Drupal*, which makes it 24.

Effects of the on-going inventory

It is recognised within the Commission that barring some omissions (caused by the scope of the 2016 inventory exercise), the list of critical software from 2016 is not likely to have changed in two years. However, this time the scope of the inventory exercise includes software development tools and resources such as commonly used libraries.

Therefore, the earlier list of critical software, plus development tools, will provide a useful input for the initial stages of software selection to satisfy the European Commission, until results from the ongoing inventory exercise can complement, or revise, the old inventories.

2.2. Other participating European Institutions

Whilst the Pilot project was primarily conducted on European Commission data, the EU-FOSSA 2 preparatory action project has been expanded its include a number of European Institutions. These include the:

1. European Parliament
2. Council of Europe
3. Council of the European Union
4. European External Action Service
5. European Economic and Social Committee and Committee of the Regions

6. European Investment Bank

The table below shows the suggested entries received from some of the Institutions. Others will contribute in due course.

Note: After internal discussions, we will highlight the software, which could be considered as potential candidates for the final list of bug bounties.

7-Zip	Adobe Acrobat Reader	Apache Maven 4.x	Apache SVN 1.9	Audacity
chromium/webkit	Eclipse (Oxygen)	Eclipse P	Eclipse Q	Eclipse Yoxos
Firefox	Forticlient	Git 2.x	Greenshot	Hexedit 3.x
iptables	JUnit 5.x	KeePass	NodeJS 10.x (Linux)	NodeJS 10.x (Windows)
Notepad ++	NSIS&NISEDIT	NXLog	PDF Creator	PuTTY
SonarQube 6.x	Talend Open Studio Data Int. 5.x	Tomcat/Jboss	tortoise	VideoLAN VLC
VLC Media Player				

2.3. The EU Public

A public survey was conducted in 2016 as part of the EU-FOSSA Pilot project. The primary software recommendations that emerged from the survey were taken into account by the project and *KeePass* was selected for a code review. However, there were a number of suggestions made, within the free text fields, and those were not considered at the time. The EU-FOSSA 2 project, with its large bug bounty programme, can consider those items.

Please find below two tables. The first shows the public proposed software that matches with the list of critical software as identified by the earlier EU-FOSSA pilot inventory exercise.

Software	Software Description	Software Type	Requested in Public Survey	Matches EC Critical List
7-Zip	File compression software	Utilities	y	y
Apache HTTP Server	Web server	Servers	y	y
Filezilla	FTP client	Utilities	y	y
Firefox	Browser	Browsers	y	y
glibc	GNU C Library	Linux/Other	y	y
KeePass	Password manager	Utilities	y	y
Linux Kernel	Core of linux	OS	y	y
OpenSSH Server	SSH Server	Linux/Other	y	y
OpenSSL	SSL Protocol	Linux/Other	y	y
PuTTY	terminal emulator, file transfer	Linux/Other	y	y

SELinux	Linux kernel security module	Linux/Other	y	y
Tomcat	Web Server	Servers	y	y
VLC Media Player	media player	Utilities	y	y
WinSCP	ftp and cloud client	Utilities	y	y

The second table below shows the rest of the EU Public proposed software. There are likely to be some matches, such as Drupal, with the on-going EU-FOSSA 2 inventory exercise.

We already know that there are items in the table that do not relate to what is installed/used at the European Institutions – the table can also be viewed as a public wish list, or an indication of areas of concern, to the section of the public that responded to the survey.

Activiti (Workflow engine)	Adium	AES Crypt	akka	AMAVISD	Apache commons-collections
Apache Commons-io	Apache commons-lang	Apache OpenOffice	Apache Xalan	Apache Xerces	Areca Backup
Bacula	bash	BIND	bitcoin	bluez	boost
BouncyCastle	Caddyserver	chromium/webkit	Clam Sentinel	ClamAV	ClamWin
Cryptomator	dbus	Debian	Debian, core system (stable)	Django	dm-crypt
Dovecot	Dropbear SSH	Drupal	ElasticSearch	Emacs	Evince
EXIM	eZ Publish	Firejail	Firmware load mechanisms	flask	Freenet Project
FreeType/libfreetype	Git client	GLPI	GNU Emacs	GnuPG	Gnutls
GoldBug	GPG4win	gunicorn	Hard drive encryption tools?	heimdal (kerberos)	HexChat
Jetty	Jitsi	Joomla	Let's Encrypt	libc	libc++
libjpeg	libjpeg-turbo	libotr	libpurple (Pidgin)	LibreOffice (office applications)	LibreSSL
liburcu	libxml2	lipng	LUKS	LXC/LXD	MariaDB
matrix.org	mime-lite	mime-lite-html	MongoDB	Moodle	musl
MySQL	namespace implementations	Network code	USB/ Firewire handlers	network stacks	SCP
NextCloud	NGINX	Node.js	NodeJS 10.x (Linux)	NodeJS 10.x (Windows)	Notepad
Notepad ++	NV Access	Open wrt	OpenBSD	Openhab	Opennebula
OpenSC	openstack	OwnCloud	Peazip	PHP	poco
POSTFIX	PostgreSQL	pwsafe	python	QGIS	Qt

quagga	RetroShare	Ruby on Rails	scp	Seafile	Signal
Spring Security	Strongswan	Suricata	systemd	TCP/IP-Stack	TeamViewer
Thunderbird	Tor	Tox	TrueCrypt	Typo3	Ubuntu
VeraCrypt	vim-tiny	Wayland	WildFly	WordPress	perl
X11	xen	xml-feed-perl	yacc	Yunohost	zcash
zlib	Zope	Zulu			

2.4. Open source software development communities

During the course of using open source software, the European Institutions have developed close links with a number of open source development communities, *Drupal* being a prime example.

Considering our relationships along with the type and amount of software we use, we consider software from the following communities to provide candidates for Bug Bounties.

- Drupal
- Apache Software Foundation
- Linux
- VLC
- KeePass (v.2.x)

2.5. Open source Development Groups within the European Institutions

Over the years of using open source software, the European Institutions have developed a wide range of software applications, many of which are open to public use. Examples include LEOS, EU Survey amongst others.

With open source software increasingly used for developing critical applications, ensuring their security is paramount. There are a number of candidates for the Bug Bounty programme, including:

- FLUX TL (DG MARE)
- DSS
- LEOS

These will be considered in the final mix.

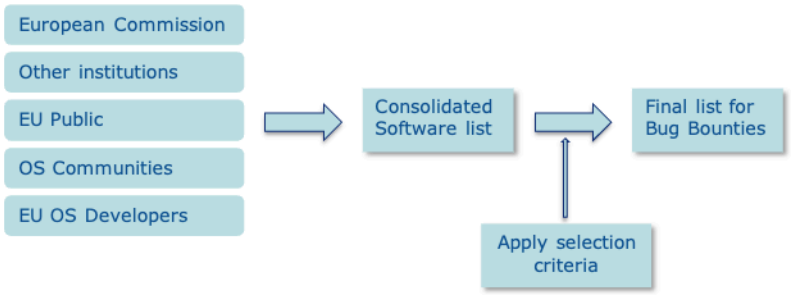
2.6. Open source software used as key building blocks

There are open source software libraries used in critical Commission's infrastructure. Two projects are being considered for bug bounties:

- midPoint (open source identity and access management library)
- WSO2 (open source enterprise platform for integrating APIs)

3. RATIONALE AND SELECTION PROCESS

Software candidates from all stakeholders will be consolidated in an excel data file. Then the agreed selection criteria will be applied, which will result in a list for bug bounties.



Selection criteria

The software selected should:

- Be of a critical nature – e.g. important to the European Institutions and damaging from a security vulnerability perspective
- Be asked for by many stakeholders if possible
- Able to benefit from Bug Bounties
- Each stakeholder should have some representation in the final list
- Have support for the audit from its developer community

The following software could, after internal discussions, be excluded:

- Well-funded, already known to be well tested software e.g. from the Mozilla foundation
- Software with little European Institutional criticality, selected only to be inclusive to other stakeholders

4. PROPOSED FINAL LIST

The EU-FOSSA 2 project proposes selecting fifteen software for bug bounties.

Need addressed	Proposed software
Front-end utilities	1. 7-zip 2. FileZilla 3. KeePass 4. VLC 5. Notepad++
Development Frameworks	6. Drupal 7. PHP Symfony
Libraries/Back-end	8. Apache Kafka 9. Glibc 10. Apache Tomcat

	11. PuTTY
EU Projects/Solutions	12. Midpoint 13. WSO2 14. DSS 15. Flux TL

END