Governance and quality of software code

Auditing of free and open-source software

An updated Inventory for the FOSS used within the European Commission*
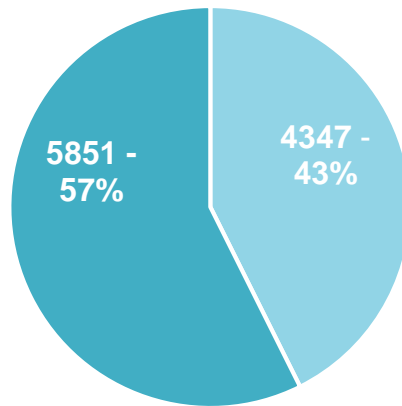
EU-FOSSA 2

May 2020

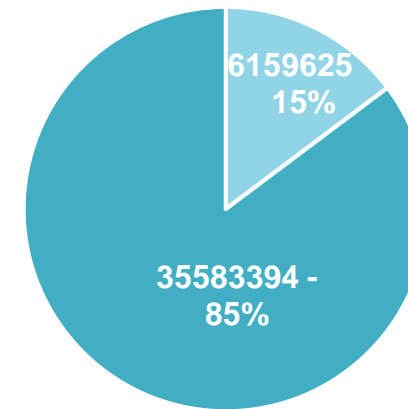* On data snapshot of December 2018

Counting and Screening FOSS

Number of software items*

5851 - 57%

4347 - 43%

Total : 10.198

■ Free and open source software ■ Other software

Number of instances*

6159625 15%

35583394 - 85%

Total : 41.743.019

* Only software items above 20 instances are estimated

■ Free and open source software ■ Other software

- Free and Open Source Software items in use at the European Commission and managed by DIGIT amount to a significant part of the total software items (4.347 out of 10.198)
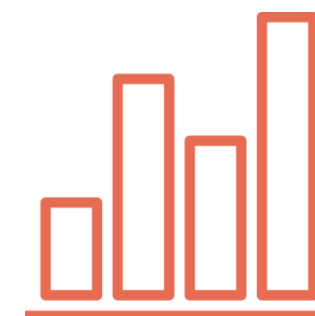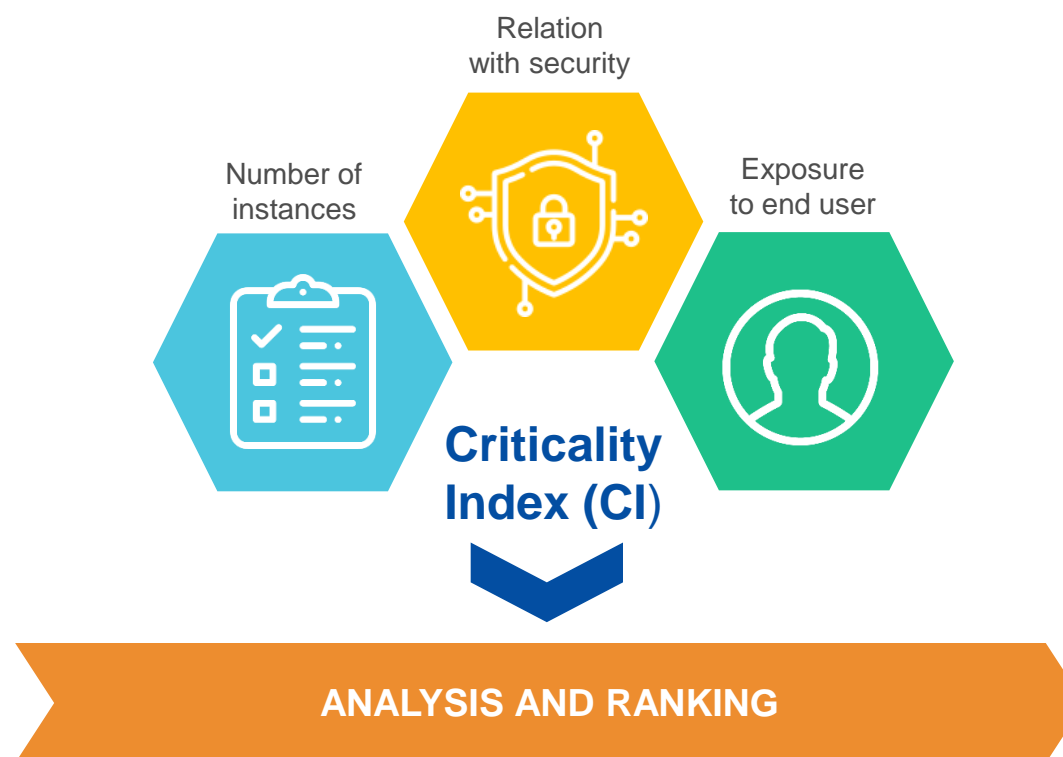- The number of instances of FOSS amounts up to 6.159.625 on a total of 41.743.019

As depicted on the graph above, 15% of all software items installed and inventoried is Free and Open Source Software

European Commission

Business criticality analysis

FOSS LIST

Software Name*	Number of instances
Java{TM} Platform SE binary	42877
Firefox	42449
VLC	39711
7-zip	37444
Perl	34192
Info-ZIP	23956
qt	22090
Calibre	20153
nspr & nss	18722
OpenSSL & pyOpenSSL	18032
glibc	17329
XULRUNNER	16529
Gecko SDK	16523
libstdc++	16073
Notepad++	14263
Python	14206
libXau	14171
bzip2	12115
Linux kernel	11791
rpm	9795

Dark grey entries indicate software names appearing for the first time

Number of instances

Relation with security

Exposure to end user

Criticality Index (CI)

ANALYSIS AND RANKING

OSS LIST RANKED BY CRITICALITY

European Commission

FOSS Criticality indexes ranking

Software	Index
QT	0.8
APACHE HTTP SERVER	0.546527841
NSPR & NSS	0.539013128
OPENSSL & PYOPENSSL	0.515527388
LIBXAU	0.456604799
APACHE TOMCAT	0.426020824
LINUX KERNEL	0.413508375
SELINUX-POLICY	0.359094613
OPENLDAP	0.356559529
OPENSSH	0.355165233
CURL	0.351090991
LIBSELINUX	0.351000453
IPTABLES	0.350710729
CYRUS-SASL	0.350583975
SVN	0.350402897
SUDO	0.350203712
PAM	0.350131281
LIBSEMANAGE	0.349606157
LIBGCRYPT	0.349551833
SHADOW-UTILS	0.348646446
M2CRYPTO	0.3485378
GLIBC	0.313789045
LIBSTDC++	0.291045722
GIT	0.233463105
RPM	0.177365324
BZIP2	0.172440018
PERL	0.168148483
SQLITE	0.161014033
PYTHON	0.157555455
LIBXML2	0.152612042
GLIB2	0.150203712
PCRE	0.149751019
ZLIB	0.149732911
LIBUSER	0.149334541
BASH	0.149244002
FIREFOX	0.6
VLC	0.37968257
JAVA	0.365226121
XULRUNNER	0.358036141
7-ZIP	0.358007458
WINSCP	0.24623769
PUTTY	0.2409695
PERL	0.23812984
FILEZILLA	0.236571374
INFO-ZIP	0.229046754
P11-KIT	0.217821972
SCP	0.216062721
GIT	0.214226982
TORTOISESVN	0.210555502
KEEPASS	0.21036428
SVN	0.204216464
TORTOISEGIT	0.201883545
GNUPG	0.20042069
CALIBRE	0.192685725
GECKO SDK	0.157978774

Partial list shown here

The critical software shortlist

For each analysed environment:

Servers

AppV & Workstations

Note: Java is not fully open source software; only source code of some libraries is available, based on a non-OSS compatible license.
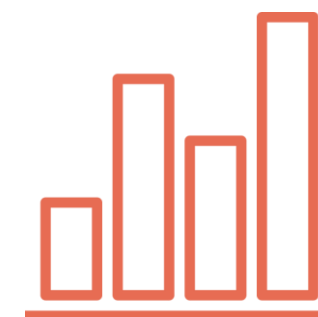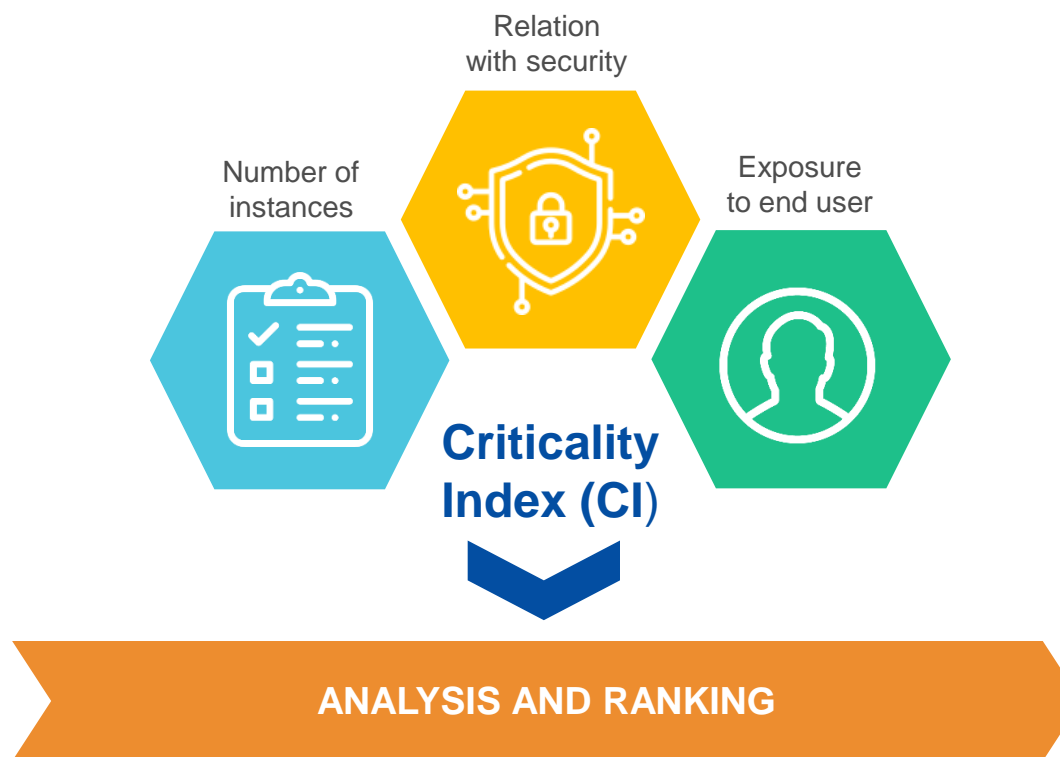
The top business critical items are sorted into a

shortlist

The vulnerabilities of the highest ranked items would impact the most due to their spread and use within the European Commission.
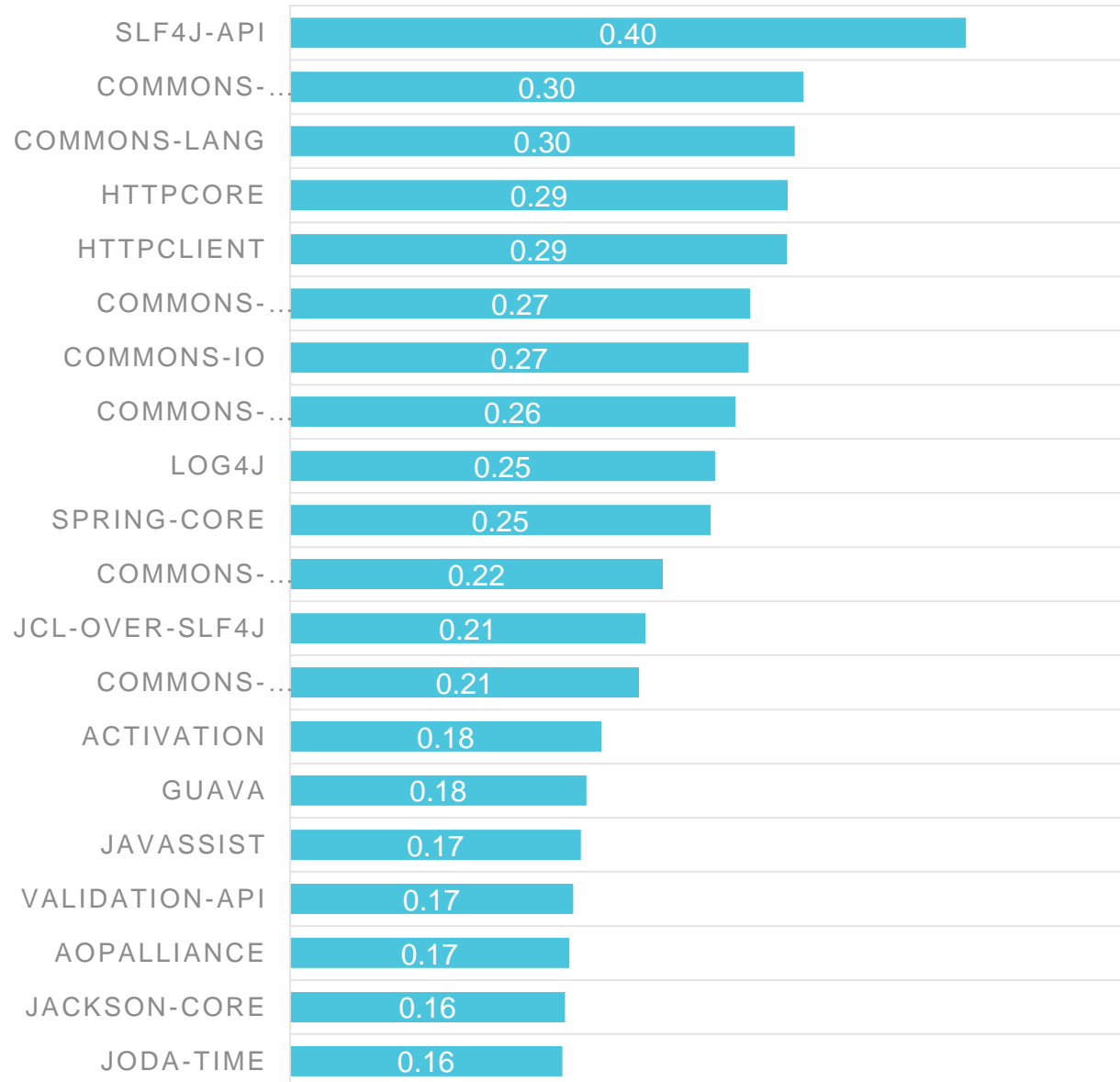
European Commission

Business criticality analysis - Nexus

FOSS LIST

Software Name	Number of Instances
slf4j-api	1672
commons-logging	1270
commons-lang	1248
commons-io	1134
commons-collections	1101
log4j	1051
spring-core	1040
commons-lang3	922
jcl-over-slf4j	879
commons-codec	863
activation	770
guava	733
javassist	719
validation-api	700
aopalliance	691
jackson-core	680
joda-time	673
jackson-databind	670
commons-beanutils	654
dom4j	638

Number of instances

Relation with security

Exposure to end user

Criticality Index (CI)

ANALYSIS AND RANKING

OSS LIST RANKED BY CRITICALITY

European Commission

NEXUS FOSS CRITICALITY RANKING

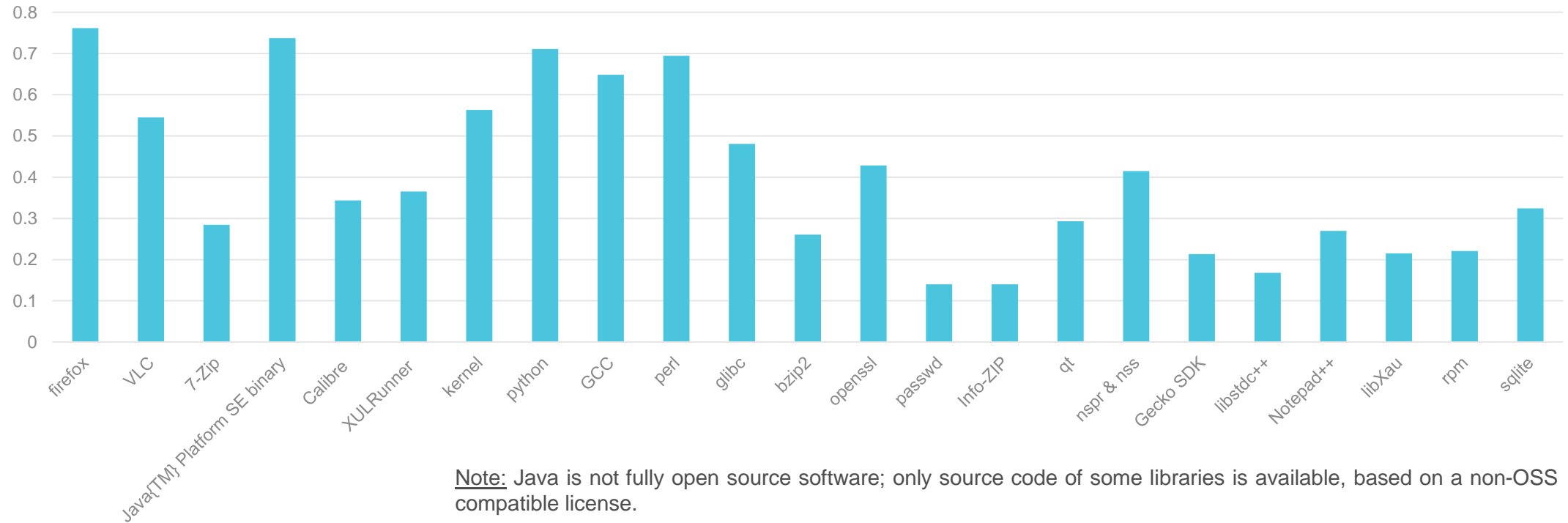|	
SLF4J-API	0.40
COMMONS-…	0.30
COMMONS-LANG	0.30
HTTPCORE	0.29
HTTPCLIENT	0.29
COMMONS-…	0.27
COMMONS-IO	0.27
COMMONS-…	0.26
LOG4J	0.25
SPRING-CORE	0.25
COMMONS-…	0.22
JCL-OVER-SLF4J	0.21
COMMONS-…	0.21
ACTIVATION	0.18
GUAVA	0.18
JAVASSIST	0.17
VALIDATION-API	0.17
AOPALLIANCE	0.17
JACKSON-CORE	0.16
JODA-TIME	0.16

Critical software shortlist - Nexus

The top business critical items inventoried in Nexus software repository are sorted into a **shortlist**

Sustainability analysis

Average of All categories that indicates overall sustainability of analysed projects

Note: Java is not fully open source software; only source code of some libraries is available, based on a non-OSS compatible license.

The critical FOSS shortlist was assessed on 34 sustainability metrics

(including Community Activity, Performance, Quality and Security, Demographics and Diversity, Governance and FOSS support.)

Sustainability analysis - Nexus

Average of all categories that indicates overall sustainability of analysed projects inventoried in the NEXUS software repository
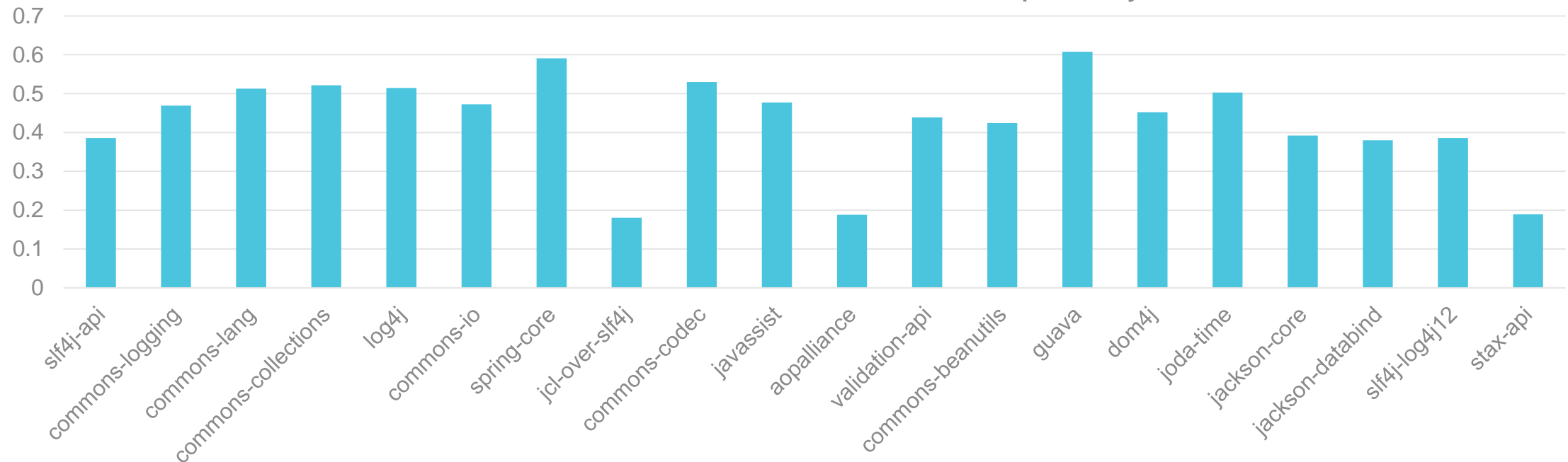
Dependency analysis

Components	Number of dependencies
Python	21 dependencies
Firefox	20 dependencies
gtk2	19 dependencies
XULRUNNER	17 dependencies
nfs-utils	15 dependencies
initscripts	14 dependencies
VLC	13 dependencies
rpm	12 dependencies
autofs	10 dependencies
subscription-manager	9 dependencies
Perl	2 dependencies

Components	Number of dependant software
Glibc	205
Bash	105
Zlib	42
coreutils	33
libselinux	32
libX11	30
systemd	28
Info	25
openssl-libs	20

The project also analysed the dependencies within the Critical FOSS shortlist. The components shown in the table have more than 1 dependency upon the shortlisted items.

The analysis shows a relative fragmentation of the dependencies, apart from Glibc and Bash, which relate to the software shown in the table.

Project Documents

For more details on the European Commission FOSS inventory, please refer to the project documents published at:

https://joinup.ec.europa.eu/collection/eu-fossa-2/eu-fossa-2-deliverables

European Commission