

The Last of the Apaches

Investigating the State of Internet-facing End-of-Life Software

Ioannis Arakas

University of Crete
& FORTH

arakas@ics.forth.gr

Panagiotis Pallis

University of Crete
& FORTH

panpas161@ics.forth.gr

Evangelos Markatos

University of Crete
& FORTH

markatos@ics.forth.gr

Georgios Smaragdakis

TU Delft

g.smaragdakis@tudelft.nl



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE



FORTH

INSTITUTE OF COMPUTER SCIENCE



TU Delft

Delft
University of
Technology

What is End of Life (EoL) and why it matters.

What is it?

We call EoL a (version of a) program that is **not supported any more** by a software vendor

Example: Windows XP and Windows 7, Apache Http 2.0

Why does it matter?

EoL software has **vulnerabilities**

EoL software can be **exploited**

EoL software will **not be patched**

Research Questions

- Q1: Are servers hosting EoL software?
- Q2: How many IP addresses out there have at least one EoL software?
- Q3: Are EoL programs dangerous?
- Q4: Where are these EoL hosts located?
- Q5: What are the factors that contribute to the high percentage of EoL programs?

Methodology (I)

We use data from Censys. Why Censys?

- frequently scans the entire IP address range
- finds open ports and applications
- reports versions of the found applications, country, hosting provider,
- range of searching options

The screenshot displays the Censys search interface. The search bar contains the query 'services.software.product='apache''. The search results are categorized into 'Hosts' with a total of 4,993,514 results and a search time of 0.53s. The interface includes a 'Host Filters' section on the left with labels such as 'remote-access' (2.72M), 'jquery' (1.08M), 'login-page' (971.04K), 'database' (748.75K), and 'email' (743.35K). The main results area shows two host entries with their respective IP addresses and associated data, including open ports and application versions.

Host Filters

Labels:

- 2.72M remote-access
- 1.08M jquery
- 971.04K login-page
- 748.75K database
- 743.35K email
- More

Autonomous System:

- 575.92K AMAZON-02
- 278.91K DIGITALOCEAN-ASN
- 217.72K AMAZON-AES

Hosts

Results: 4,993,514 Time: 0.53s

136.127.58.242 (ip-247-96-124-136.us-east-1b.amazonaws.com)

136.200.164.1 (ip-164-151-136.us-east-1b.amazonaws.com)


Methodology (II)

EoL application information available at endoflife.date for a large number of programs and version.

Apache HTTP Server

APACHE SERVER-APP WEB-SERVER

Last updated on 26 July 2024

 [Apache HTTP Server](#) is a collaborative software development effort aimed at creating a robust, commercial-grade, feature-rich and freely available source code implementation of an HTTP (Web) server.

Release	Released	Security Support	Latest
2.4	12 years ago (21 Feb 2012)	Yes	2.4.62 (17 Jul 2024)
2.2	18 years ago (01 Dec 2005)	Ended 7 years ago (11 Jul 2017)	2.2.34 (11 Jul 2017)
2.0	22 years ago (05 Apr 2002)	Ended 11 years ago (10 Jul 2013)	2.0.65 (09 Jul 2013)

Methodology (III)



Software	Latest Version	EoL Date	EoL Version	EoL Date
Apache http	2.4	unknown	2.2	Jul 2017
Nginx	1.27	unknown	1.26	Apr 2024
OpenSSL	3.3	Apr 2026	1.1	Sep 2023
PHP	8.3	Dec 2027	8.0	Nov 2023
MySQL	9.0	unknown	8.3	Apr 2024
MariaDB	11.5	unknown	10.10	Nov 2023
Squid	6	unknown	5	Jul 2023



Results

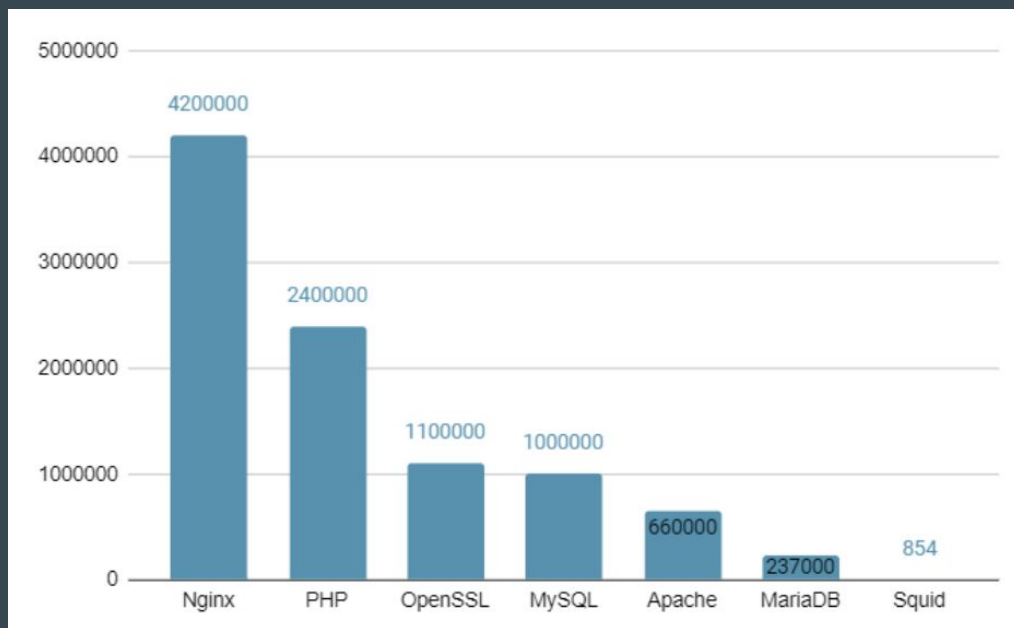
Q1: Are servers hosting EoL software?

Our research has shown that:

46 millions IP addresses host at least one of the software that we studied.

Unfortunately 9.6 millions IP addresses **hosts at least one EoL** program/software.

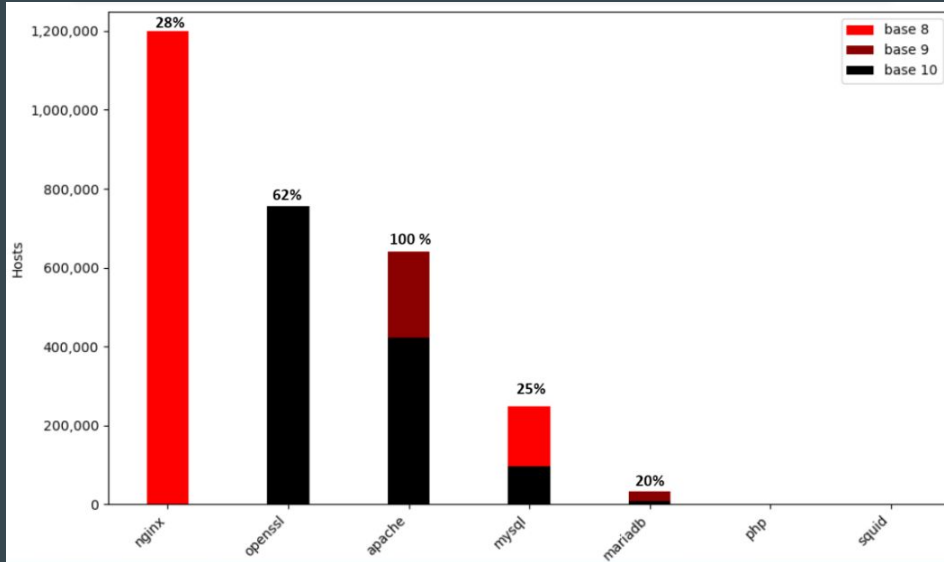
Q2: Do servers host EoL software?



- More than 4 million IP addresses run EoL Nginx.
- More than 2 million IP addresses run EoL PHP.

Number of Hosts that run at least on EoL Software

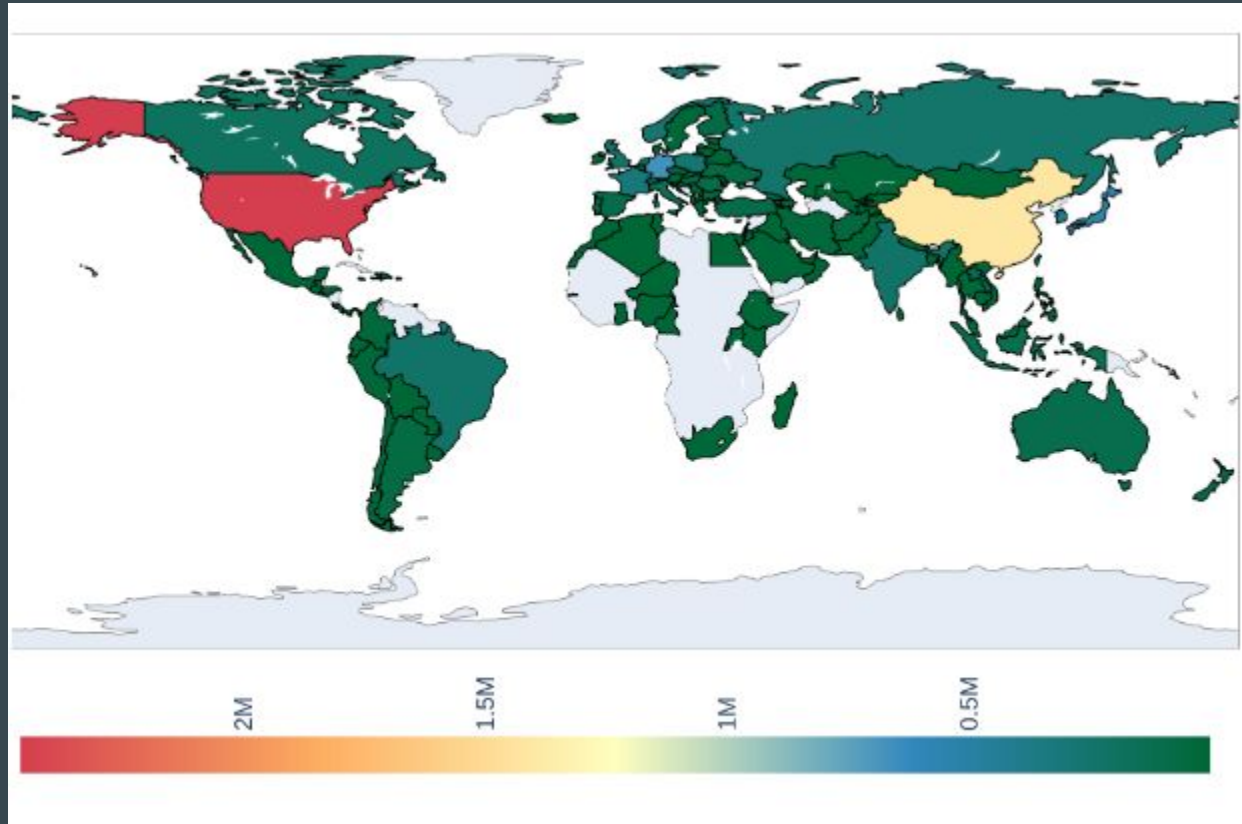
Q3: Are EoL applications dangerous?



- **All of the** apache instances are EoL and **vulnerable (CVE with high score >8)**
- One in four nginx servers have CVE higher than 8

EoL Hosts with at least one CVE with base score higher or equal to eight nine or ten

Q4: Where are these EoL hosts located?



Q5: What are the factors that contribute to the high percentage of EoL programs?

Operating System (OS)	Release Date	Hosts	OpenSSL Version	End of Openssl Support
Ubuntu 20.04	Apr 2020	1,349,000	1.1.1f	Sep 2023
Debian 10	Jul 2019	542,000	1.1.1n	Sep 2023
Ubuntu 18.04	Apr 2018	482,000	1.1.1f	Sep 2023
Ubuntu 16.04	Apr 2016	362,000	1.0.2g	Dec 2019
Debian 9	Jun 2017	316,000	1.1.0k	Sep 2019
Ubuntu 14.04	Apr 2014	112,000	1.0.1f	Dec 2019
Opensuse Leap 42.1	Nov 2015	4,800	1.02k	Dec 2019

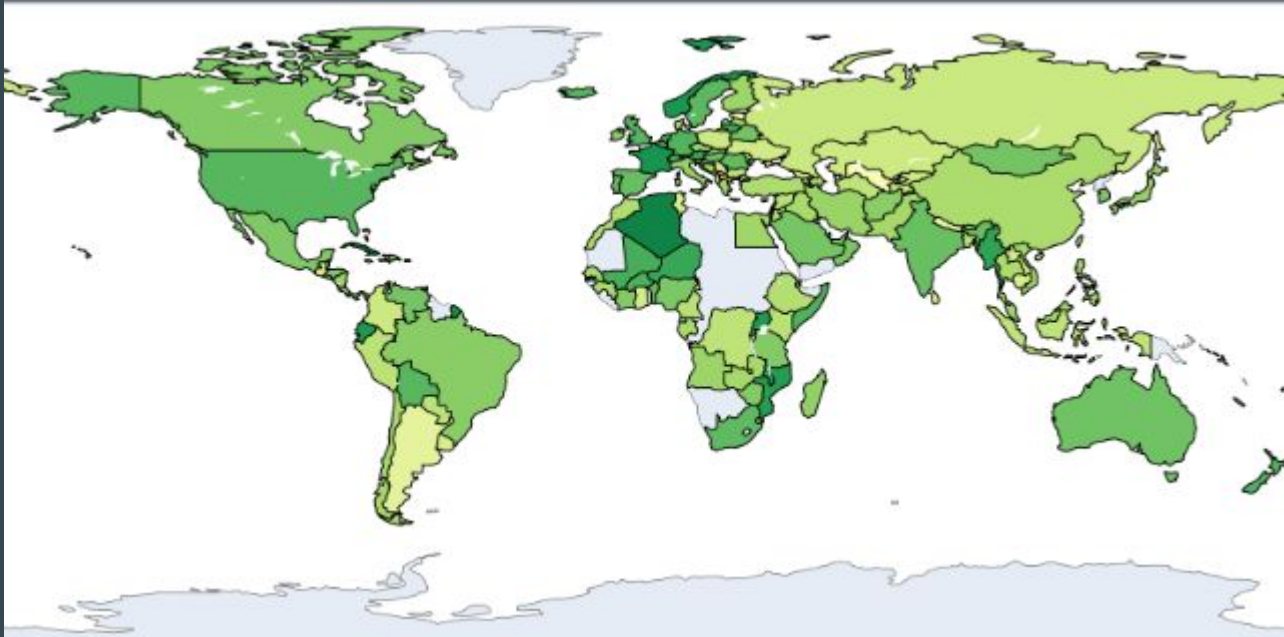
Conclusions - summary

- More than 9 million IP addresses run EoL software.
- All of the EoL apache instances are vulnerable with high base score.
- Almost 800,000 OpenSSL instances are EoL and vulnerable with high base score.
- Pre-installed software shipped with OS might be EoL.

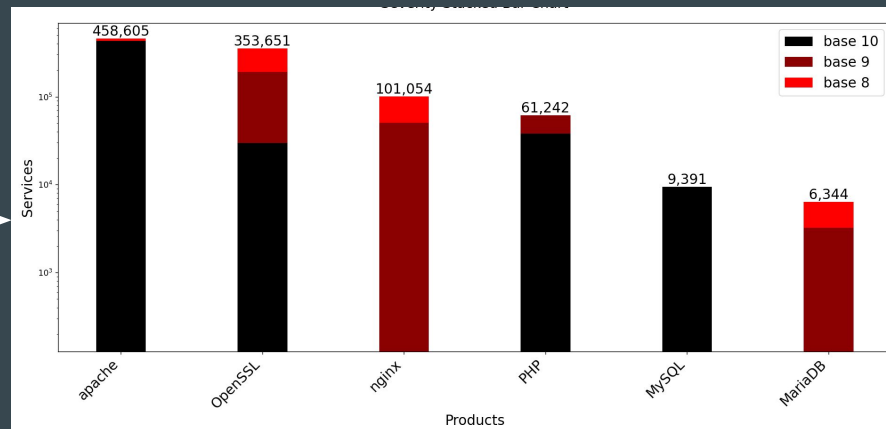
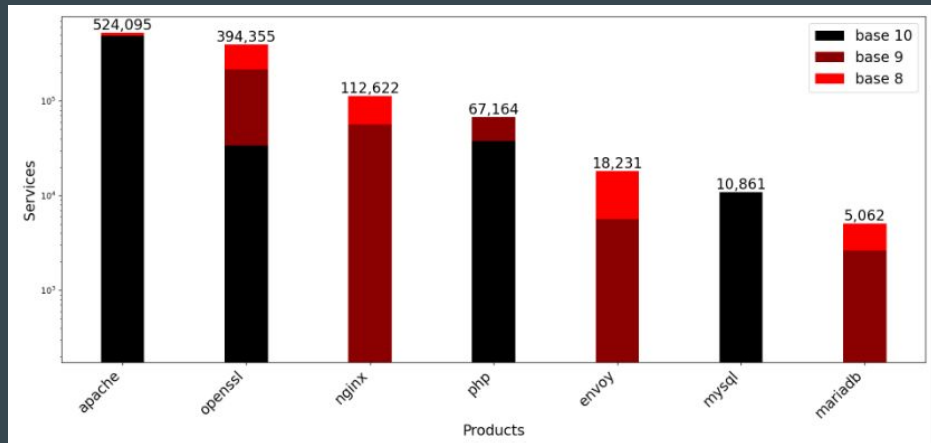
- Recommendations:
 - Update your software.
 - Don't use the preinstalled version of a tool: update it
 - Use only supported programs for better patching.

Thank You

Q4: Where are these EoL hosts located
(percentage)



Is EoL software dangerous. (May 2024, Oct 2024)



NPM Weekly downloads (Oct 2024)

Weekly Downloads

