The Last of the Apaches: Investigating the State of Internet-facing End-of-Life Software

Ioannis Arakas
arakas@csd.uoc.gr
FORTH-ICS and University of Crete
Greece

Panagiotis Pallis
panpas161@gmail.com
FORTH-ICS and University of Crete
Greece

Evangelos Markatos
markatos@ics.forth.gr
FORTH-ICS and University of Crete
Greece

Georgios Smaragdakis
g.smaragdakis@tudelft.nl
Delft University of Technology
The Netherlands

Abstract

In the software development life-cycle, new software packages are deployed while older ones are phased out as they reach their "End of Life" and are no longer supported. Despite this lack of support, some of these End-of-Life (EoL) software distributions are still popular and are being used. However, running EoL software poses massive security risks as older software may contain vulnerabilities for which security updates are no longer available. In this paper we investigate the prevalence of EoL software in Internet-facing devices. To our surprise, we find that more than 6 million out of the 44.3 million hosts we consider in our study are running at least one EoL version of very popular software, including web server software, software libraries, databases, and scripting languages.

In addition, NIST identifies some of these EoL versions as highly vulnerable and highly or critically severe (severity score higher than 7 and 9 respectively). To identify which networks are at greater risk, we investigate regions and networks with a high concentration of hosts running EoL software. Our work aims to raise awareness within both the research and operational communities about the current state of End-of-Life (EoL) software and the potential risks associated with its continued large-scale use.

CCS Concepts

• **Security and privacy** → **Software security engineering**; **Web application security**; • **Networks** → *Network security*.

Keywords

End-of-Life Software, Common Vulnerabilities and Exposures.

ACM Reference Format:
Ioannis Arakas, Panagiotis Pallis, Evangelos Markatos, and Georgios Smaragdakis. 2026. The Last of the Apaches: Investigating the State of Internet-facing End-of-Life Software. In *19th European Workshop on Systems Security (EuroSec '26), April 27–30, 2026, Edinburgh, Scotland, UK.*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3803525.3804984

EuroSec '26, Edinburgh, Scotland, UK.

ACM ISBN 979-8-4007-2603-3/26/04
https://doi.org/10.1145/3803525.3804984

1 Introduction

Over the past few years, software product development has steadily increased. Indeed, according to recent studies [30], the global software market is anticipated to reach around US$1.8 trillion by 2032, poised to grow at a compound annual growth rate (CAGR) of 11.74% between now and 2032. In addition to commercial software produced by corporations, open/free software development is also increasing rapidly. For instance, GitHub, which hosts over 100 million developers, has been experiencing rapid growth, roughly doubling its user base every 2.5 years [17].

Unfortunately, the rapid pace of software development also brings certain challenges. One notable challenge is the trend toward shorter software life-cycles and reduced support periods for software products. In addition, mergers, bankruptcies, and acquisitions of companies may provide even shorter support for existing software products. And to make matters worse, open-source projects may be discontinued because they lack sufficient developers to maintain them. As a result, several software packages soon reach their *End-of-Life* (EoL), i.e., they are no longer supported after a specified date. Despite this lack of support, EoL software distributions may remain popular and continue to run even after official support has ended. Unfortunately, running EoL software may lead to significant security risks [13, 33], as it may contain exploitable vulnerabilities for which users will likely not receive security patches.

On the positive side, regulatory intervention by the US National Institute of Standards and Technology (NIST) [28, 34], the US Cybersecurity and Infrastructure Security Agency (CISA) [33], and the European Commission [16] have made significant steps towards reducing this problem. The European Commission, in particular, recently introduced the Cyber Resilience Act (CRA) [15], which proposes very strict rules for software vendors concerning the support they will provide for their software. According to the CRA, manufacturers are required to provide security updates for a minimum of five years or for the expected duration of the product's use, whichever is longer.

While the CRA clearly promotes active manufacturer support for systems, our findings indicate that many Internet-facing systems in use lack such support and are already at the end of their lifespans. In this paper, we quantify the current Internet exposure of End-of-Life

(EoL) software, i.e., software versions that no longer receive vendor or upstream security updates. Using Internet-wide scan data, we measure how many Internet-facing servers run EoL software and what fraction of them are associated with known vulnerabilities for which no patch is, or will be, available.
Our contributions can be summarized as follows:

- We examine 6 widely used software products that are currently installed and running on over 44.3 million Internet-facing servers worldwide. Our analysis reveals that at least 6 million IPv4-reachable hosts we measure run at least one EoL version across six popular stacks (Apache HTTP Server, Nginx, PHP, MySQL, MariaDB, Squid).
- Widely used software on Internet-facing hosts (such as Nginx, PHP, and Apache HTTP) are often running unsupported, End-of-Life (EoL) versions that are vulnerable to cyber attacks. In fact, 523.301 hosts using an EoL Apache have at least one potential vulnerability (CVE) that the U.S. National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) has classified as critical (with a severity score of 9 or higher). These servers are at significant risk of being compromised — if they haven't already been.
- 60.91% (1.96 M) of PHP hosts use an EoL version that is no longer supported and is vulnerable to cyberattacks. At the same time, 3,563,956 hosts are using an EoL version of Nginx.
- When we turn our attention to the regional and network characteristics of Internet-facing servers, we observe variation across multi-tenant cloud providers, but overall, these prefixes are not systematically associated with lower EoL software prevalence relative to the cross-AS average.
- Our findings reveal that millions of hosts (IP addresses) run operating systems that have been unsupported for many years. For example, 50% of EoL Ubuntu hosts have been out of support for nearly 2 years, while 264,000 Windows Server hosts are running versions that reached end of life over 17 years ago.
- We show that many of the very popular stable server software distributions, e.g., Ubuntu, Debian, and CentOS, use modules that are no longer supported by their vendors, unintentionally increasing the number of Internet-facing servers running EoL software.
- The artifacts of this study, including the queries used in Censys and the scripts used to correlate EndOfLife.date with other data sources to infer hosts running end-of-life software, are publicly available on GitHub [3].

Our work is intended to make the research and operational communities aware of the current state of EoL and the potential risks of continuing to operate EoL software at this scale. We hope our study will be a call to action towards reducing the EoL software installations on Internet-facing servers towards a safer Internet for all.

2 Data Sources

In this section, we discuss the software we consider in our study and the sources we utilize to identify their versions.

2.1 Popular Server Software

In our study, we focus on several server software products that are widely used in application development and are commonly deployed on Internet-facing servers serving millions—if not billions—of end users. Our selection was based on data from both Censys [5, 8] and endoflife.date [14]. In future work, we will study a broader range of tools in order to generalize the results.
The tools used in our study are:
PHP is a general-purpose scripting language that is especially suited to web development.
Apache HTTP Server, also known as "httpd", is an open-source HTTP server for modern operating systems including UNIX and Windows.
MariaDB is an open source relational database and it provides an SQL interface for accessing data.
MySQL is an open-source relational database management system.
Nginx is an HTTP web server, reverse proxy, content cache, load balancer, TCP/UDP proxy server, and mail proxy server.
Squid is a caching proxy for the Web that supports HTTP, HTTPS, FTP, and more.

2.2 End-of-Life Software Information

End-of-Life (EoL) information is challenging to track, as it is typically provided by the software vendor on its website and does not follow any standard representation or format. In our analysis, we bootstrap our investigation by using `endoflife.date` [14] (an API that collects EoL information for software). We also use cvedetails [7], which provides all the subversions for each tool. Subversions are necessary to query Censys and correlate a tool's exact version with a Common Vulnerabilities and Exposures (CVEs).

2.3 Scanning Data

In our study, we use data from Censys [5], accessed via their respective APIs. We chose to rely on the Censys API, as the APIs of other scanning datasets, e.g., Shodan, provide data for only a subset of tools. Indeed, we were able to query only Nginx and Apache using Shodan, and we also confirmed that Censys offers better scanning coverage and accuracy [11]. Unless otherwise stated, our analysis is based on Censys data obtained under a research license. We note that Censys follows the best practices of a good Internet citizen [31]. It announces the IPs used for scanning [4] and also uses reverse PTR records to redirect to a webpage that reveals their identity. When they receive a request to exempt IP ranges from the scan, their portals honor it. Thus, in our study, parts of the publicly advertised Internet may not be scanned upon the owner's request for the associated address space.

3 End-of-Life Analysis

In this section, we evaluate the global landscape of servers running End-of-Life (EoL) software, with a breakdown by individual software products. We also examine the associated security risks and explore the underlying factors that contribute to the continued use of EoL software on these servers.

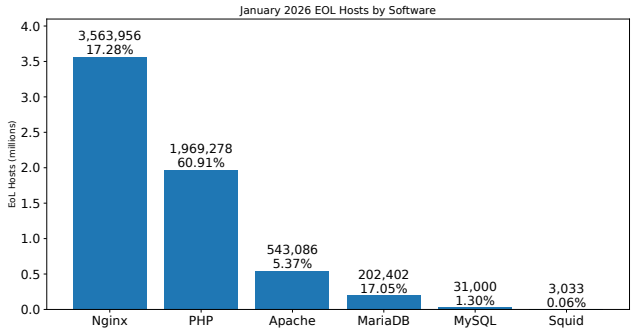

Figure 1: Hosts with at least one instance of EoL software in January 2026. This figure shows the software with the highest EoL number. In the first place by raw numbers we see Nginx 17.28% of its hosts running EoL software which amount to more than million hosts. But percentage wise PHP is first with 60.91% (1.96 million hosts) of the hosts running an EoL version.

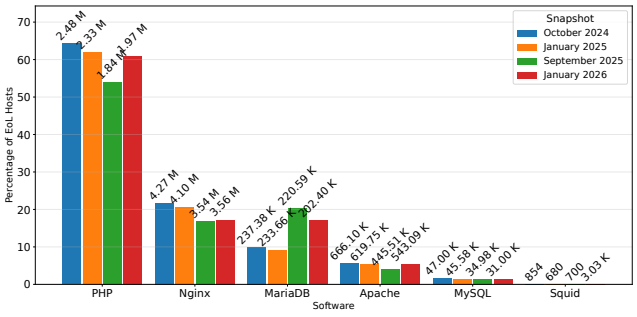

Figure 2: Percentage of Hosts with at least one instance of EoL software. Snapshots were taken in October 2024, January 2025, September 2025 and January of 2026 .

3.1 Baseline Results

In Figure 1, we plot the number of installations identified in January 2026 as EoL based on Censys scans. A host may run multiple products (e.g., Apache HTTP Server and PHP) from our study, but when counting the overall results, we ensure we count only unique hosts. We found that 3,563,956 Nginx hosts (17.28%) and 1,969,278 PHP hosts (60.91%) are EoL. On the other hand, we find that 31,000 MySQL hosts are EoL out of a total of 2,390,445 hosts.

3.2 Snapshots

In Figure 2, we captured four snapshots of the data: October 2024, January 2025, September 2025, and January 2026. These snapshots illustrate how Internet-exposed EoL software evolved over roughly one year. Rather than showing a steady decline, the data reveal a mixed pattern; some software decreases through September 2025, while others remain stable or worsen, with several categories increasing again by January 2026. This variation is partly explained by software releases that transition to end-of-life status during the observation period.

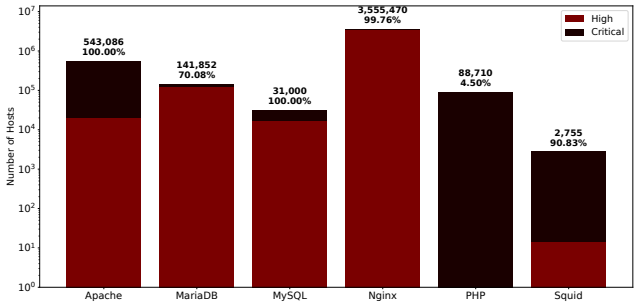

Figure 3: Count of hosts running end-of-life (EoL) software with at least one CVE rated 7 or higher. Snapshot was taken in January 2026. There are 543,086 (EoL) Apache HTTP hosts with all of them having at least one CVE exceeding a score of 7 and 523.301 of which include a CVE that are rated at 9.8.

3.3 Vulnerability Severity Level

While our analysis indicates that the use of EoL software is widespread, especially for popular and critical products such as Apache, Nginx, PHP, and MySQL, it remains unclear to what extent this exposure results in actual vulnerability exploitation. To investigate this further, in Figure 3, we plot the number of hosts that are characterized at least "high risk" by the U.S. National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) and Exposures database [26], i.e., they are tagged with a CVE category based on the severity score (High 7.0–8.9; Critical 9.0 - 10). These CVEs also have a high exploitability score, indicating strong potential for real-world exploitation and a lower barrier to adversaries weaponizing them.

To correlate EoL Hosts with specific CVEs, we used the exact version of a tool with known vulnerabilities to match that version. This indeed shows a *potential* vulnerability. It is worth mentioning that a vulnerability patch is usually included in the next minor release of the software. Meaning that the services mentioned above, unless manually patched, are probably vulnerable and susceptible to attacks. Finally, most of the potentially vulnerable hosts not only run software with a CVE and a high base severity score, but those CVEs also have a high *exploitability* score, which measures how easily a vulnerability can be attacked.

In our measurements 100% of the EoL Apache httpd hosts are associated with at least one High (7-9) and 523.301 of them with a Critical (9+) CVE . Similar trends are observed in MariaDB, MySQL, Nginx, and Squid software.

3.4 Regional Characteristics

Next, we focus on the regional characteristics of hosts that run EoL software. To illustrate these characteristics, in Figure 4, we plot the total number of identified hosts per country that run at least one of the six main software products considered in our study. As the plot shows, the hosts are not evenly distributed across countries. For example, the USA has the most (10.6 million) hosts running at least one of the 6 main software products. China is second, with 3.4 million hosts, and Germany is third, with 3.1 million hosts.

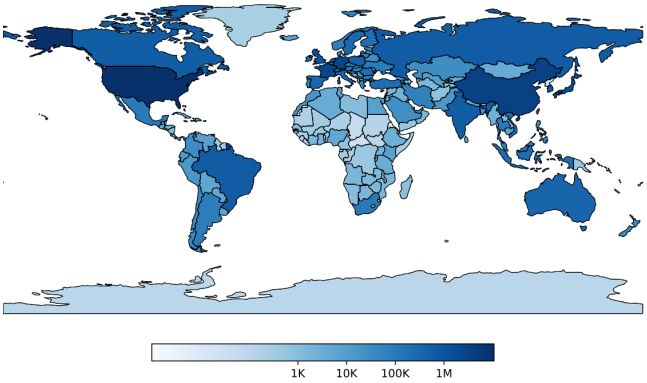

Figure 4: World map: Number of hosts with at least one instance of the software products Apache, Nginx, PHP, squid, Mysql and MariaDB (stable and EoL versions) . United States of America is first with 10.6M Hosts followed by China with 3.4 million Hosts. The data were taken in September 2025.

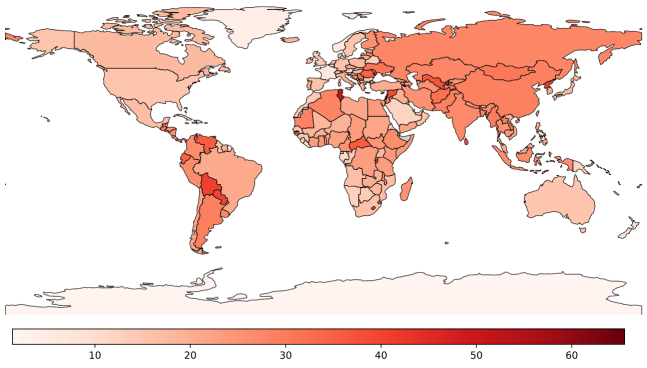

Figure 5: World map: Percentage of hosts with at least one EoL software (Apache, Nginx, PHP, squid, Mysql, and MariaDB). United States of America has an overall percentage of 15.4 of EoL Hosts, France has 6.5 , Germany has 25.2 , Russia has 27.8 and China has 28.6. The data were taken in September 2025.

In Figure 5, we show the percentage of EoL hosts in those countries that run at least one of the six main software products considered in our study. The results reveal a clear divide between wealthier and less affluent countries in terms of EoL software usage. Overall, countries in Asia have the worst numbers, followed by countries in South America and Africa. China and Russia have 28.6% and 27.8%, respectively. On the other hand, the United States has an overall percentage of 15.4 and more hosts than any other country, as shown in Figure 4. Similarly, most European countries have a lower overall percentage, with France, the United Kingdom, and the Netherlands at 6.5, 14.0, and 14.6, respectively.

3.5 Business Characteristics

In Table 1, we examine End-of-Life (EoL) prevalence in the address space of several large and widely used cloud, hosting, and service providers, e.g., Amazon AWS, Digital Ocean, OVH, and service providers and content delivery networks, e.g., Google, Cloudflare, Microsoft. Although globally, around 4.12% of servers running Apache HTTP Server use an EoL version, the percentage in cloud providers is lower (excluding Cloudflare). However, for server applications like Nginx, the percentage of servers that run EoL software is very high, as high or even higher than the average globally. We should note that not all Nginx versions are associated with high-severity CVEs. Nevertheless, some of the versions are high-risk and have not been upgraded to supported versions. Our analysis shows high variability regarding MariaDB, Nginx, and PHP. Percentages differ across providers, so we conclude that there is no strong correlation between the autonomous system and the EoL percentage.

AS No	Name	Apache	PHP	Nginx	Squid	MySQL	MariaDB
16509	Amazon O2	2.00%	61.03%	24.22%	1.06%	0.54%	20.93%
14061	Digital Ocean	1.34%	45.14%	29.60%	-	1.36%	29.22%
16276	OVH	2.51%	49.21%	27.65%	0.01%	2.31%	27.35%
14618	Amazon Aes	1.71%	59.91%	25.99%	0.25%	0.57%	18.40%
396982	Google Cloud Platform	0.79%	51.49%	30.85%	-	0.75%	40.84%
8075	Microsoft Corp	0.79%	50.22%	14.59%	-	1.23%	30.79%
37963	Alibaba Advertising	4.46%	54.28%	30.96%	-	1.11%	43.52%
45102	Alibaba US Technology	2.69%	54.49%	25.12%	-	0.78%	40.09%
15169	Google LLC	0.05%	61.87%	22.85%	-	-	-
209242	Cloudflare	10.40%	92.26%	13.77%	-	3.54%	21.48%
*	AS Average	4.12%	53.88%	16.86%	0.01%	1.37%	20.39%

Table 1: Percentage of EoL software in popular cloud providers – Apache Httpd, PHP, Nginx, Squid, MySQL and MariaDB (September 2025). "–" indicates that we did not observe any hosts running the corresponding software product in that provider's address space.

Server OS	Release Date	End of OS Support	Hosts	Openssl Version	End of Official Openssl Support
Ubuntu 20.04	Apr 2020	May 2025	1.6 M	1.1.1f-1ubuntu2.24	Sep 2023
Debian 10	Jul 2019	Sep 2022	753 K	1.1.1n-0+deb10u3	Sep 2023
Ubuntu 18.04	Apr 2018	May 2023	911 K	1.1.1f-1ubuntu2.1 18.04.23	Sep 2023
Ubuntu 16.04	Apr 2016	Apr 2021	506 K	1.0.2g-1ubuntu4.20	Dec 2019
Debian 9	Jun 2017	Jul 2020	374 K	1.1.0k-1 deb9u1	Sep 2019
Ubuntu 14.04	Apr 2014	Apr 2019	128 K	1.0.1f-1ubuntu2.27	Dec 2019

Table 2: Pre-installed openssl versions on EoL and Stable popular Server OS versions. Snapshot of Hosts was taken in January of 2025. We see that there are more than 128k thousand of Hosts that are running ubuntu. This operating system has expired as well as the openssl version and the expanded security support.

3.6 Server Software Distributions

In Figure 6 we plot the CDF of popular server operating systems (OSes). Surprisingly, we observed that many widely used operating systems have not been supported for years. Over 500,000 Ubuntu servers are running unsupported versions. Notably, Ubuntu 18.04, which had been out of support for nearly two years at the time of our analysis, is still in use on more than 346,000 hosts. Moreover, 10% out of all EoL Ubuntu hosts have been unsupported for more than 5 years, so even the extended security maintenance has expired. Additionally, over 7% of EoL Windows Server hosts are running versions that expired 17 years ago. Other popular operating systems, such as Debian and CentOS, exhibit similar End-of-Life patterns to those seen with Ubuntu.

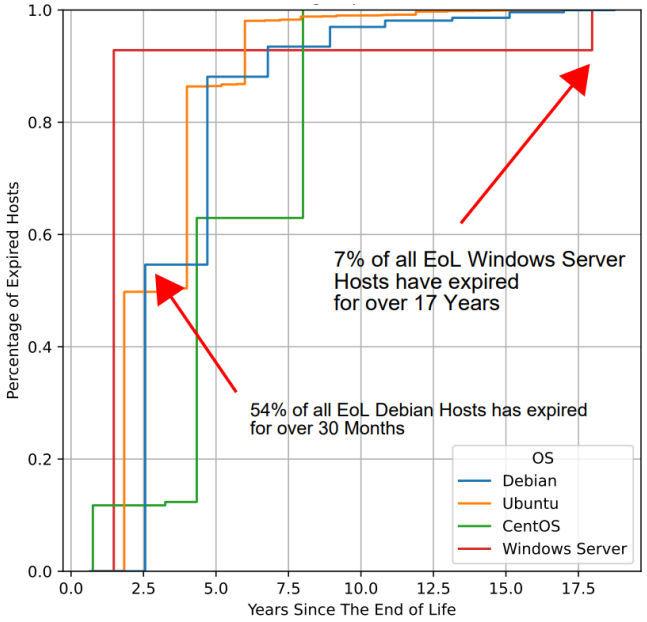

Figure 6: CDF plot of hosts with expired Operating System. The x-axis represents the number of years since the operating system reached end-of-life (EoL), while the y-axis indicates the fraction of the total expired systems. We observe that, among the hundreds of thousands of expired Ubuntu and Debian servers, over 50% have been unsupported for more than two years. This figure only includes hosts that are EoL.

During our study, we also observed that many OS releases (stable and EoL), e.g., Ubuntu 20.04, use EoL versions, such as OpenSSL 1.1.1, which is upstream EoL. This and other releases of OpenSSL (see Table 2) are no longer supported by OpenSSL. Vendor support continues by backporting security fixes for OpenSSL and other critical components into older releases. However, there might be some risk. First of all, receiving these fixes after the standard support time window requires manual configuration: attaching an Ubuntu Pro token and enabling the legacy ESM service. Second, even the vendor's extended support is set to end after some years, leaving thousands of running hosts with unsupported software.

4 Discussion

Based on our study's results, we recommend policies for software updates. We also discuss the limitations of this study.

4.1 Policy Recommendations

To address the growing risks posed by outdated and unsupported software, we propose a set of new policies to enhance transparency and long-term maintainability. First, companies should be legally required to publicly disclose the EoL dates for all software products. For that, it is crucial to adopt a standardized format such as `EndOfLife.date` [14] for easy public access and integration. Second, legislation should mandate a minimum number of years of post-release software maintenance, ensuring users are not left without support. Although the Cyber Resilience Act[1] in the EU is a positive step towards this direction, it should be adopted in other areas of the world. Third, when major version upgrades are not backward-compatible, vendors must provide tools or scripts to facilitate migration. Fourth, if a product is discontinued, its owners should make every effort to open-source it. This will allow the product to continue being updated and maintained through community support.

4.2 Labeling and Versioning Data

To count hosts with at least one EoL tool as accurately as possible, we query Censys for the tool and its exact version. For example, we search for Nginx 1.22.1. Then, we consider all hosts with an unlabeled version to be stable. This clearly leaves many unlabeled EoL versions uncounted. We therefore under-report the issue. As mentioned before, we use cvedetails to gather all the tool subversions. This exposed us to mistakes made by CVE details. In September 2025, while collecting data, the EoL versions 1.22.*, 1.24.*, 1.26.*, and 1.27.* were missing. This led to an underestimation of EoL Nginx hosts by 3 million, as we later discovered. To maintain consistency, we did not consider these versions. As a result, we knowingly underestimated the problem.

4.2.1 Host Vulnerabilities. In accordance with ethical guidelines, we did not attempt to exploit the identified hosts to confirm vulnerabilities or gain access to them. Instead, we report that these hosts are potentially vulnerable based on the data and tools we used. It is nearly impossible to test millions of hosts across a wide variety of CVEs and software stacks, as such a process cannot be fully automated to the extent of proving our hypothesis. We acknowledge that banners may not always provide sufficient evidence for vulnerable hosts, and additional testing is needed to confirm that hosts are vulnerable to specific CVEs [21].

We would like to emphasize that our research focuses on explaining why outdated software should not be used, rather than analyzing why so many hosts remain vulnerable. Our work is also meant to inform policymakers, researchers, and engineers about the current state of Internet-facing software.

4.2.2 Honeypots. Some of the servers we collect may be honeypots. While there is no definitive figure for the proportion of Internet-facing servers that are honeypots, some estimates place it as high as 15–25% [27]. Even under this conservative assumption, at least 75% of the servers we identified are likely not honeypots.

4.2.3 Extended Security Maintenance. Operating systems like Ubuntu offer Extended Security Maintenance (ESM) to continue providing critical security updates for versions that have reached the end of their standard support period. While standard Ubuntu LTS releases receive 5 years of free security updates, ESM extends this support by an additional 5 years, for a total of 10 years of security maintenance. Similarly, Red Hat provides 5 years of support, while Debian offers 2 years.

In our research, we cannot determine which operating systems have ESM enabled. But we know ESM is not enabled by default, meaning that system owners must manually activate it—assuming

[1] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

they are aware of its existence. As shown in Figure 6, more than 55% of Debian End-of-Life (EoL) hosts have been unstable for over 2 years. This suggests that even if ESM had been enabled initially, it would no longer be supported. Similarly, we observe that around 10% of EoL Ubuntu systems have passed the end of their ESM.

4.3 Scanning Data Limitations

Our analysis is limited to the publicly observable state of the internet as captured by Censys. We cannot assess non-public-facing systems, which may have a different security posture, whether better or worse. We rely on version information provided by Censys. This data may not indicate whether a software instance was patched without a version change or an explicit update. To categorize our findings as EoL or stable, we use collected banners and protocol-level scanning. Our matching is one-to-one, meaning we look for exact product matches to determine if a host is EoL. As a result, we probably under-report the EoL population.

4.4 Ethical Considerations

The research in this paper does not raise any ethical issues. In our study, we did not explore any vulnerabilities, and we relied mostly on active measurements available to us via an educational license. We will not release the list of vulnerable IPs. We are in the process of informing the cloud providers of EoL or vulnerable hosts about our findings.

In our testing, we observe that Shodan provided a smaller number of IP addresses but with a significantly higher rate of IP(s) per server (IP/s) containing at least one EoL service. While Censys reported a higher rate of IP/s, with a smaller number of those ip/s running some EoL software. Given Censys's higher IP address coverage, more conservative results, and more advanced query syntax, compared to Shodan and others (e.g., Hunter), for the rest of the paper, unless specified, we will analyze the Censys dataset.

5 Related Work

Large-scale Internet measurement studies have been widely used to assess the state of the web. Among these, our work can be framed as an active Internet-wide study augmented with longitudinal snapshots [29].In recent years, Internet-wide scanning has become increasingly accessible through community-driven tools [9, 18, 19] and commercial search engines such as Censys [5] and Shodan [32]. Censys has commercialized high-speed scanning technologies—such as ZMap [13] and variants [1, 22, 23]—capable of scanning the entire Internet in minutes and detecting services across any port. Their vantage points are deployed at multiple geographic locations on the Internet, providing better coverage of the server deployment. This deployment is difficult to achieve when utilizing one or a limited number of vantage points. Censys [5] provides a comprehensive view of hosts and networks on the Internet, including details about SSL certificates, domains, and open ports.

Shodan [32] covers a wide range of Internet-connected devices, including webcams, routers, servers, and more. It provides detailed information about devices, including banners, open ports, services running, and sometimes even vulnerabilities. It also offers monitoring capabilities to track changes and updates to devices of interest. In a recent empirical paper [11], the creators of Censys demonstrated that it outperforms all other major scanning platforms, making it more efficient at uncovering services running on hosts.

Wang et al. [35, 36] are also studying the state of the internet regarding EoL software, but they mostly focus on embedded devices. Our work has a broader scope, covering all types of EoL software and revealing even more EoL and potentially vulnerable hosts. A similar work by Lauinger et al. [24] focuses on the state of vulnerable JavaScript commonly found in the frontend of popular websites. Durumeric et al. [13] provided a characterization of misissued certificates and a case study identifying 3.4 million devices running UPnP versions with known vulnerabilities. Follow-up studies also performed large-scale scanning to estimate the number of servers vulnerable to Heartbleed [12], invalid SSL certificates [6], stale TLS certificates [25], mismanagement of networks [37], or routers with critical vulnerabilities [2, 10], shortcomings in routing protocols [20]. However, apart from some anecdotes, there has been no systematic study of the state of Internet-facing hosts, especially servers, that run End-of-Life software.

6 Conclusion

In this paper, we investigate how many Internet-facing devices run End-of-Life software, i.e., software no longer officially supported and for which patches are unavailable. We consider 6 popular server applications, ranging from server software to secure communication libraries and databases. To our surprise, at least 6 million of the 44.3 million hosts that run at least one of these software packages rely on EoL versions. Given that EoL software is known to be vulnerable, we also show that a significant fraction of these hosts are potentially at high risk. We present the demographics of servers running EoL software globally and by software product. Our results also show that EoL software is run on cloud providers' infrastructure.

Our work is not just an observation, but a crucial call to action for the research and operational communities. We aim to raise awareness about the current state of EoL software and the potential risks associated with its continued operation at this scale. We hope that our study will inspire a collective effort to significantly reduce the number of EoL software installations on Internet-facing servers, helping to ensure a safer Internet.

This study focuses on a small set of tools as an initial step. In future work, we will expand our dataset to include a broader range of tools to generalize the results, while also examining each tool more deeply to identify trends.

Acknowledgment

We are grateful to Censys and Shodan for providing us research access to their datasets. This work was funded by the European Union C-SOC grant number 8515915, and under the Horizon Europe Programme as part of the projects SafeHorizon (#101168562) and RECITALS (#101168490). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

References

[1] David Adrian, Zakir Durumeric, Gulshan Singh, and J Alex Halderman. 2014. Zippier ZMap: Internet-wide Scanning at 10 Gbps. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*.

[2] Aniket Anand, Michalis Kallitsis, Jackson Sippe, and Alberto Dainotti. 2023. Aggressive Internet-wide Scanners: Network Impact and Longitudinal Characterization. In *ACM CoNEXT*.

[3] John Arakas and Panagiotis Pallis. 2026. The Last of the Apaches. https://github.com/johnarakas/The-Last-of-the-Apaches. GitHub repository, accessed 2026-03-23.

[4] Censys. 2024. Opt Out of Data Collection. https://support.censys.io/hc/en-us/articles/360043177092-Opt-Out-of-Data-Collection.

[5] Censys. 2024. The Censys Platform. https://censys.com/.

[6] Taejoong Chung, Yabing Liu, David Choffnes, Dave Levin, Bruce MacDowell Maggs, Alan Mislove, and Christo Wilson. 2016. Measuring and Applying Invalid SSL Certificates: The Silent Majority. In *Proceedings of the Internet Measurement Conference*.

[7] CVE Details. 2026. CVE Details: Vulnerability Statistics and Information. https://www.cvedetails.com/. https://www.cvedetails.com/ Accessed: 2026-01-29.

[8] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman. 2015. A Search Engine Backed by Internet-Wide Scanning. In *CCS*.

[9] Zakir Durumeric, David Adrian, Phillip Stephens, Eric Wustrow, and J Alex Halderman. 2024. Ten Years of ZMap. In *Proceedings of the Internet Measurement Conference*.

[10] Zakir Durumeric, Michael Bailey, and J Alex Halderman. 2014. An Internet-Wide view of Internet-Wide Scanning. In *23rd USENIX Security Symposium*.

[11] Zakir Durumeric, Hudson Clark, Jeff Cody, Elliot Cubit, Matt Ellison, Liz Izhikevich, and Ariana Mirian. 2025. Censys: A Map of Internet Hosts and Services. In *ACM SIGCOMM*.

[12] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, et al. 2014. The Matter of Heartbleed. In *Proceedings of the Internet Measurement Conference*.

[13] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-Wide Scanning and its Security Applications. In *USENIX Security Symposium*.

[14] Endoflife.date. 2024. Endoflife.date Website. https://endoflife.date/.

[15] European Commission. 2024. EU Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[16] European Union Agency for Cybersecurity (ENISA). 2023. Threat Landscape Report 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[17] Github. 2023. 100 million developers and counting. https://github.blog/2023-01-25-100-million-developers-and-counting/.

[18] Robert David Graham. 2014. MASSCAN: Mass IP port scanner. *URL: https://github.com/robertdavidgraham/masscan* (2014).

[19] Harm Griffioen, Georgios Koursiounis, Georgios Smaragdakis, and Christian Doerr. 2024. Have you SYN me? characterizing ten years of Internet scanning. In *Proceedings of the IMC*.

[20] Tomas Hlavacek, Italo Cunha, Yossi Gilad, Amir Herzberg, Ethan Katz-Bassett, Michael Schapira, and Haya Shulman. 2020. DISCO: Sidestepping RPKI's Deployment Barriers. In *Network and Distributed System Security Symposium (NDSS)*.

[21] Szu-Chun Huang, Harm Griffioen, Max van der Horst, Georgios Smaragdakis, Michel van Eeten, and Yury Zhauniarovich. 2025. Trust but Verify: An Assessment of Vulnerability Tagging Services. In *USENIX Security Symposium*. Seattle, WA.

[22] Liz Izhikevich, Renata Teixeira, and Zakir Durumeric. 2021. LZR: Identifying Unexpected Internet Services. In *30th USENIX Security Symposium (USENIX Security 21)*.

[23] Liz Izhikevich, Renata Teixeira, and Zakir Durumeric. 2022. Predicting IPv4 Services Across All ports. In *Proceedings of the ACM SIGCOMM 2022 Conference*. 503–515.

[24] Tobias Lauinger, Abdelberi Chaabane, Sajjad Arshad, William Robertson, Christo Wilson, and Engin Kirda. 2018. Thou shalt not depend on me: Analysing the use of outdated javascript libraries on the web. *arXiv preprint arXiv:1811.00918* (2018).

[25] Zane Ma, Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric, Michael D Bailey, Angelos D Keromytis, Fabian Monrose, and Manos Antonakakis. 2023. Stale TLS Certificates: Investigating Precarious Third-party Access to valid TLS keys. In *Proceedings of the Internet Measurement Conference*.

[26] MITRE. 2024. MITRE Common Vulnerabilities and Exposures database. https://cve.mitre.org/.

[27] Martin Mladenov, Laszlo Erdodi, and Georgios Smaragdakis. 2025. Uncovering Exposed Industrial Control Systems and Honeypots. In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroSP)*.

[28] National Institute of Standards and Technology. 2011. Managing Information: Security Risk Organization, Mission, and Information System View. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf.

[29] Morteza Safaei Pour, Christelle Nader, Kurt Friday, and Elias Bou-Harb. 2023. A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security* 128 (2023), 103123.

[30] Precedence Research. 2022. Software Market Forecast 2023-2032. https://www.precedenceresearch.com/software-market.

[31] Philipp Richter and Arthur Berger. 2019. Scanning the scanners: Sensing the internet from a massively distributed network telescope. In *Proceedings of the Internet Measurement Conference*. 144–157.

[32] Shodan. 2024. Search Engine for the Internet of Everything. https://www.shodan.io/.

[33] U.S. Cybersecurity and Infrastructure Security Agency (CISA). 2023. Understanding Patches and Software Updates. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates.

[34] U.S. Cybersecurity and Infrastructure Security Agency (CISA). 2024. Protect Your Business by Updating Your Software. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates.

[35] Dingding Wang, Muhui Jiang, Rui Chang, Yajin Zhou, Baolei Hou, Xiapu Luo, Lei Wu, and Kui Ren. 2021. A measurement study on the (in) security of end-of-life (eol) embedded devices. *arXiv preprint arXiv:2105.14298* (2021).

[36] Dingding Wang, Muhui Jiang, Rui Chang, Yajin Zhou, Hexiang Wang, Baolei Hou, Lei Wu, and Xiapu Luo. 2023. An empirical study on the insecurity of end-of-life (EoL) IoT devices. *IEEE Transactions on Dependable and Secure Computing* 21, 4 (2023), 3501–3514.

[37] Jing Zhang, Zakir Durumeric, Michael D Bailey, Mingyan Liu, and Manish Karir. 2014. On the Mismanagement and Maliciousness of Networks. In *Network and Distributed System Security Symposium*.