CVEs With a CVSS Score Greater Than or Equal to 9

Lena Sinterhauf [1,2], Andreas Aßmuth [2], and Roland Kaltefleiter [1]
[1] NetUSE AG, Kiel, Germany
e-mail: {lsi | rk}@netuse.de
[2] Kiel University of Applied Sciences, Kiel, Germany
e-mail: andreas.assmuth@haw-kiel.de

***Abstract*—Critical vulnerabilities with Common Vulnerability Scoring System scores of 9.0 or higher pose severe risks to organisations' information systems. Timely detection and remediation are essential to minimise economic and reputational damage from cyberattacks. This paper provides a thorough analysis of the identification and resolution timelines of such critical vulnerabilities. A mixed-methods approach is employed, integrating quantitative data from global vulnerability databases analysing 245,456 Common Vulnerabilities and Exposures records spanning from 2009 to 2024, of which 12.8 % were critical, with qualitative case studies of notable incidents. This methodical combination of quantitative and qualitative data sources enables the identification of patterns and delay factors in vulnerability management. The findings indicate significant delays in public disclosure and patch deployment, influenced by industry-specific factors, resource availability and organisational processes. The paper concludes with a series of actionable recommendations to improve the efficiency of vulnerability responses. Despite faster disclosure, the remediation gap for critical vulnerabilities remains a systemic risk, driven by organisational inertia and system complexity.**

Keywords-critical vulnerabilities; vulnerability detection time; vulnerability management; patch management.

I. Introduction

The increasing digitisation and interconnectivity of organisations and critical infrastructures has led to a growing threat landscape dominated by cyberattacks. Information security constitutes a central component within contemporary corporate strategies, with the objective of preserving the integrity, availability, and confidentiality of data. The standardised identification and documentation of security vulnerabilities is facilitated by the Common Vulnerabilities and Exposures (CVE) system [1]. The assessment of vulnerabilities is conducted through the utilisation of the Common Vulnerability Scoring System (CVSS), a method that employs a scale ranging from 0 (lowest) to 10 (highest) to evaluate the severity of the vulnerabilities identified [2]. Vulnerabilities that receive a score of 9.0 or higher are designated as critical, given the substantial risks they pose to the affected systems.

Despite the implementation of established security processes, the timely detection and remediation of critical vulnerabilities remain challenging. The failure to disclose vulnerabilities or the failure to deploy patches in a timely manner can expose organisations to significant risks of exploitation, resulting in financial losses, operational disruptions and reputational damage [3][4]. Notable incidents, such as the Log4Shell vulnerability, have underscored the pressing need for effective and efficient vulnerability management [5]–[7].

The present study investigates the speed and efficiency of identifying and remediating critical vulnerabilities, focusing on those with CVSS scores of 9.0 or above. It synthesises quantitative analyses of vulnerability data from global databases spanning 2009 to 2024 with qualitative case studies of major security incidents. The objective of this study is to identify the factors that contribute to delays in vulnerability response and to provide actionable recommendations for improving the resilience of IT infrastructures against critical security threats.

This study provides a long-term analysis of critical vulnerabilities (CVSS ≥ 9.0) across 245,456 CVE records over a period of 16 years (2009 to 2024). Contrary to previous studies, this research combines large-scale quantitative analysis with qualitative case studies of major incidents (Heartbleed, EternalBlue, and Log4Shell) to identify systemic delays in vulnerability remediation and examines sector-specific patch patterns across more than 20 industries, thus providing practical insights for the prioritisation of vulnerability remediation in the context of limited security resources.

The structure of this paper is as follows: Section II provides a comprehensive review of the extant literature on vulnerability management and scoring systems. Section III delineates the research methodology. The fourth section of this text presents the results of the data analyses and case studies. The subsequent section, Section V, discusses the implications of these findings. Finally, Section VI concludes with a summary and suggestions for future research.

II. Related work

Research on software vulnerabilities has addressed the subjects of detection, severity assessment, and remediation. CVSS a widely utilised numerical classification system for vulnerability criticality, which serves to guide the prioritisation of remediation efforts [2][8]. Service Level Agreements (SLAs) have been proposed as a means of defining remediation timelines. It is recommended that critical vulnerabilities be addressed within days to weeks [9][10].

Empirical studies have analysed vulnerability lifecycles, management frameworks, open-source processes, and metrics, such as mean time to remediate and disclosure-to-patch delays [11][12]. The extant literature consistently highlights challenges in the timely remediation of issues, which are influenced by system complexity, organisational readiness, and resource constraints.

Research focusing explicitly on critical vulnerabilities reports that, despite improvements in disclosure speed, patch

TABLE I. RELATED WORK ON CVE/CVSS ANALYSIS (2009 TO 2025)

Year	Title	Author(s)	Topics
2019	Practical patch management and mitigation	S. Alexiou	Patch SLAs, remediation timelines [10]
2022	Guide to enterprise patch management planning	M. Souppaya, K. Scarfone	MTTR metrics, enterprise patching [11]
2025	To patch or not to patch	J.R.C. Nurse	Patching motivations, organisational challenges [12]
2025	The secret life of CVEs	P. Przymus et al.	CVE lifecycle analysis [13]
2025	Out of sight, still at risk	P. Przymus et al.	Transitive vulnerabilities, Maven ecosystem [14]

deployment often lags behind, thereby extending exposure windows and exploitation risk [13][14]. Despite the existence of regulatory and sector-specific guidelines that advocate for faster responses, the efficacy of patching varies across sectors and vendors.

Key studies on vulnerability management and CVE lifecycles have been summarised in Table I. Whilst the extant literature provides insights into patching processes and vulnerability lifecycles, none offer a long-term (2009 to 2024) analysis focused on critical vulnerabilities (CVSS ≥ 9.0) across sectors, combined with qualitative case studies of high-impact incidents. The present study addresses this gap by integrating large-scale quantitative data with detailed case analyses to uncover patterns, delays, and factors unique to the highest severity vulnerabilities.

III. METHODS

The present study employs a mixed-methods approach in order to comprehensively analyse the identification and remediation processes of critical security vulnerabilities. The methodology integrates quantitative analysis of vulnerability data with qualitative case studies to gain both breadth and depth of understanding.

The quantitative component employs data from recognised vulnerability databases, namely the National Vulnerability Database (NVD) and the MITRE CVE database [15][16]. The data were obtained from the official NVD JSON 2.0 feeds (as of 28 May 2025) and MITRE CVE list downloads (as of 20 May 2025). The datasets were processed using Python scripts (e.g., *pandas*, *json*) to filter vulnerabilities with CVSS base scores of ≥ 9.0, to calculate temporal metrics (e.g., days from *reservation_date* to *published* and to *lastModifiedDate* as patch proxy), and to aggregate results by year, assignee (assigners), and sector.

The analysis encompasses $245{,}456$ CVE records registered between January 2009 and December 2024, of which $31{,}430$ (approx. $12.8\,\%$) were classified as critical with CVSS base scores of 9.0 or higher. Two primary temporal dimensions were examined: the duration from CVE reservation to public disclosure, and the duration from disclosure to patch availability (approximated using database modification timestamps). Statistical analysis was conducted to examine these timelines, identify trends and patterns over time, and reveal discrepancies across industry sectors and software categories.

The qualitative element of the study comprises in-depth case studies of notable security incidents, including the Heartbleed, EternalBlue, and Log4Shell vulnerabilities [6][17][18]. The case studies presented offer insights into the challenges encountered by organisations in the field of vulnerability management, including issues, such as delays, organisational factors, and best practices in mitigation.

The integration of quantitative and qualitative data facilitates cross-validation and more profound interpretation of results. Quantitative findings reveal statistical trends and potential delay factors, while qualitative analysis contextualises these findings within actual incident scenarios and management practices.

The process of data validation entailed several key steps. Firstly, database entries were subjected to rigorous cross-checking. Secondly, the results were meticulously compared with existing literature to ensure the reliability of the findings. Finally, consistency was maintained throughout all analysis phases. This integrated approach facilitates the development of pragmatic recommendations that are designed to enhance the efficiency and effectiveness of critical vulnerability management.

IV. RESULTS

The analysis encompasses vulnerability data from 2009 to 2024, with a particular emphasis on critical vulnerabilities that have a severity score of 9.0 or higher. The results of the study reveal three primary dimensions of interest: detection and publication timelines, patch availability delays, and organisational or sectoral variation in response times.

A. Detection and Publication Timelines

The total number of registered vulnerabilities increased substantially over the study period, particularly after 2016 when the CVE assignment process was expanded through the introduction of CVE Numbering Authorities (CNAs) [19][20], as illustrated in Figure 1.

In this context, “registrations” denote the initial allocation of a CVE ID by MITRE or designated CNAs upon internal vulnerability reporting, prior to public disclosure [21][22]. “Publications” refer to the subsequent public release of detailed

vulnerability information in databases, such as MITRE and the NVD, making it visible to the global security community [21]–[23].

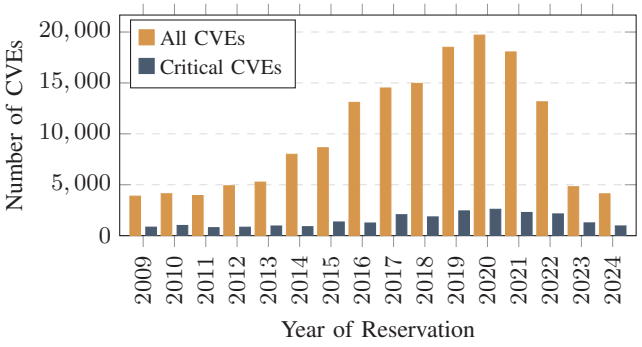

Figure 1. Annual distribution of CVE registrations (2009–2024). Orange bars represent total no. of CVEs, while blue bars show no. of critical vulnerabilities.

This phenomenon resulted in a marked increase in the publication of vulnerabilities in 2017 and again during the period of the pandemic caused by the virus known as SARS-CoV-2 (2020–2021), when working remotely and accelerated digitisation led to a greater number of exposed systems (cf. Figure 2).

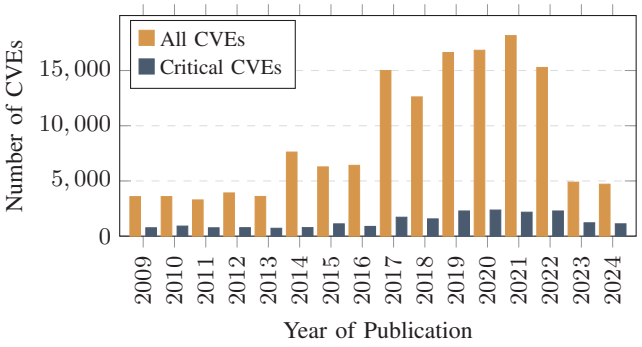

Figure 2. Annual distribution of CVE publications (2009–2024). Orange bars represent total no. of CVEs, while blue bars show no. of critical vulnerabilities.

The proportion of critical vulnerabilities remained relatively stable throughout the observation period at approximately 12.8 % of all registered CVEs, with a peak of 2,589 cases recorded in 2020. As illustrated in Figure 3, the average time from CVE reservation to public disclosure has decreased dramatically, from over 400 days in 2013 to approximately 33 days in 2024.

Notably, while critical vulnerabilities were published significantly faster than the overall average in earlier years (e.g., 57 vs. 105 days in 2009), this gap has virtually disappeared in recent years, indicating that systematic improvements in disclosure processes now benefit all vulnerability severity levels equally. This convergence represents a positive development in the CVE ecosystem. Nevertheless, the CVSS remains essential for severity classification and prioritisation, particularly when organisations face resource constraints or must process large

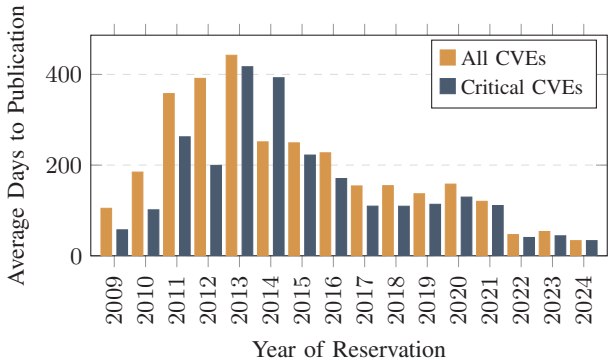

Figure 3. Average time from CVE reservation to public disclosure (2009–2024). Orange bars represent all CVEs, while blue bars show critical vulnerabilities.

numbers of vulnerabilities simultaneously, making it advisable to address critical issues first.

Our investigations also revealed that the time between registration and publication of a vulnerability varies considerably. While in some cases, assigners published registered CVEs on the same day (duration 0 days), in other cases it took up to several years. Of course, the reasons for these enormous differences in time are not apparent from the data available to us. In cases where the time span is very short, immediate publication is usually due to already known or simultaneously published vulnerabilities that were subsequently assigned a CVE ID. However, short time spans also indicate that some organisations appear to have particularly efficient processes in place, possibly automated disclosure procedures or internal Standard Operating Procedures (SOPs) that prioritise rapid publication. Long durations do not automatically mean that poor work was done in these cases. Reasons for this can also include complex coordination processes, late discovery of the actual impact, or subsequent publication of confidential vulnerabilities [23][24].

Notably, none of the assigners have an average publication time of 0 days for critical CVEs. This indicates that critical vulnerabilities are always subjected to at least a brief review before they are made public. Furthermore, it can be observed that the longest average delay for critical CVEs (approx. 850 days) is significantly shorter than for all CVEs (over 2,300 days). This suggests that critical vulnerabilities are generally processed and published more quickly, even when delays occur. At the same time, the data shows that the variance in duration for critical CVEs is lower, suggesting increased process standardisation or prioritisation.

B. Time to Patch Availability

Patch deployment analysis demonstrates that turnaround times are both longer and more variable than those observed in the publication phase. The mean time to release a patch for general vulnerabilities was approximately 1,732 days (median: 1,335 days), whereas for critical vulnerabilities it was around 2,024 days (median: 1,668 days).

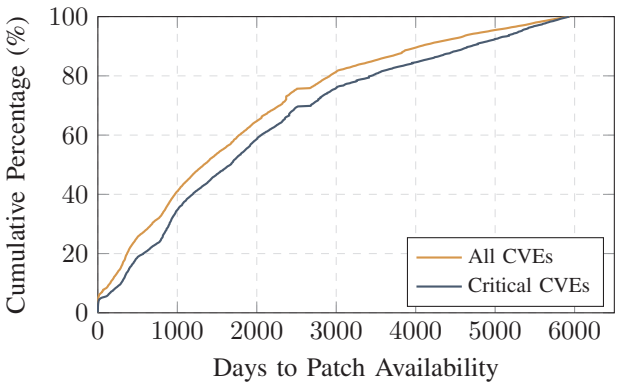

Figure 4. Cumulative distribution of time to patch availability (2009–2024). The curves show the percentage of CVEs patched within a given timeframe. Mean values: approximately 1,732 days (all CVEs) and 2,024 days (critical CVEs).

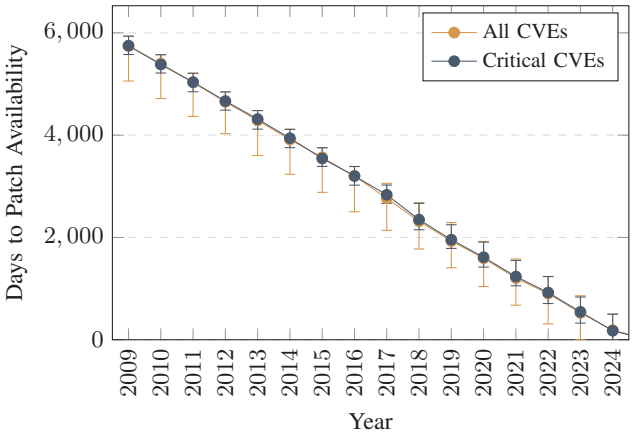

Figure 5. Patch availability for all CVEs and critical CVEs (2009–2024). The average, minimum and maximum durations are specified for each year. In the trend lines, the orange line indicates all CVEs, while the blue line indicates critical CVEs.

Figure 4 illustrates the cumulative distribution of time to patch availability across the entire observation period. Notably, 50 % of all CVEs received patches within 1,335 days of disclosure, while 90 % were patched within 4,054 days. For critical vulnerabilities, the corresponding values were 1,668 and 4,689 days. The distribution demonstrates that despite prioritisation efforts, critical vulnerabilities exhibit longer remediation times on average than the general population, likely reflecting the increased complexity and coordination requirements associated with high-severity issues. The highly skewed distribution, with substantial differences between median and mean values, indicates that while the majority of vulnerabilities are addressed within reasonable timeframes, a significant tail of delayed patches persists across both categories.

Despite the improvements that have been made, no consistent or significant difference has been demonstrated between critical and non-critical issues with regard to patch completion times, as can be seen in Figure 5. The apparent improvement in recent years should be interpreted with caution due to right-censoring: vulnerabilities from 2022 onwards have had less opportunity to exhibit extended patch delays, and currently unpatched vulnerabilities are not represented in these measurements.

Many organisations implement release cycles that are similar across all severity levels. The phenomenon of extended exposure periods can be attributed to various factors, including the increasing complexity of systems, the presence of legacy dependencies, constraints in resources, and the incomplete automation of processes. However, between 2020 and 2024, an observable acceleration occurred, suggesting stronger regulatory and procedural pressure on vendors.

C. Organizational and Sectoral Variations

There are notable disparities between different assignees (assigners). It is evident that certain entities, including specialised security platforms and prominent open-source providers, attained a median patch time of less than five days. This is indicative of sophisticated automation and continuous integration processes. In contrast, slower assigners – which were often commercial software vendors — exhibited median delays of between 2,000 and 4,000 days (cf. Figure 6).

Sectors were assigned by mapping CVE assigners to primary industry classifications using a reproducible, rule-based keyword matching on assigner names, with overlaps between sectors (e.g., Open Source, Commercial Software, Web & Content Management) resolved through a predefined prioritisation order. While this heuristic facilitates large-scale mapping, multi-sector entities and evolving business models may introduce classification uncertainties.

TABLE II. NUMBER OF ALL AND CRITICAL CVES BY SECTOR.

Sector	All CVEs	Critical CVEs
Cloud & Hosting	3700	263
Commercial Software	41583	4658
Consulting & Research	82386	15744
Consumer Electronics	55	9
Education & Non-Profit	33	4
Finance & Insurance	66	2
Hardware	13474	1276
Healthcare	22	10
Industrial & IoT	2493	308
Open Source	28699	2751
Other	51873	4055
Platforms & DevOps	108	1
Security Vendors	7249	848
Telecommunication & Networking	13620	1476
Web & Content Management	95	25

While sample sizes vary considerably across sectors (Table II), the median-based analysis remains robust for identifying general remediation patterns, with smaller sectors (e.g., Healthcare, $n = 22$) providing indicative trends rather than definitive benchmarks.

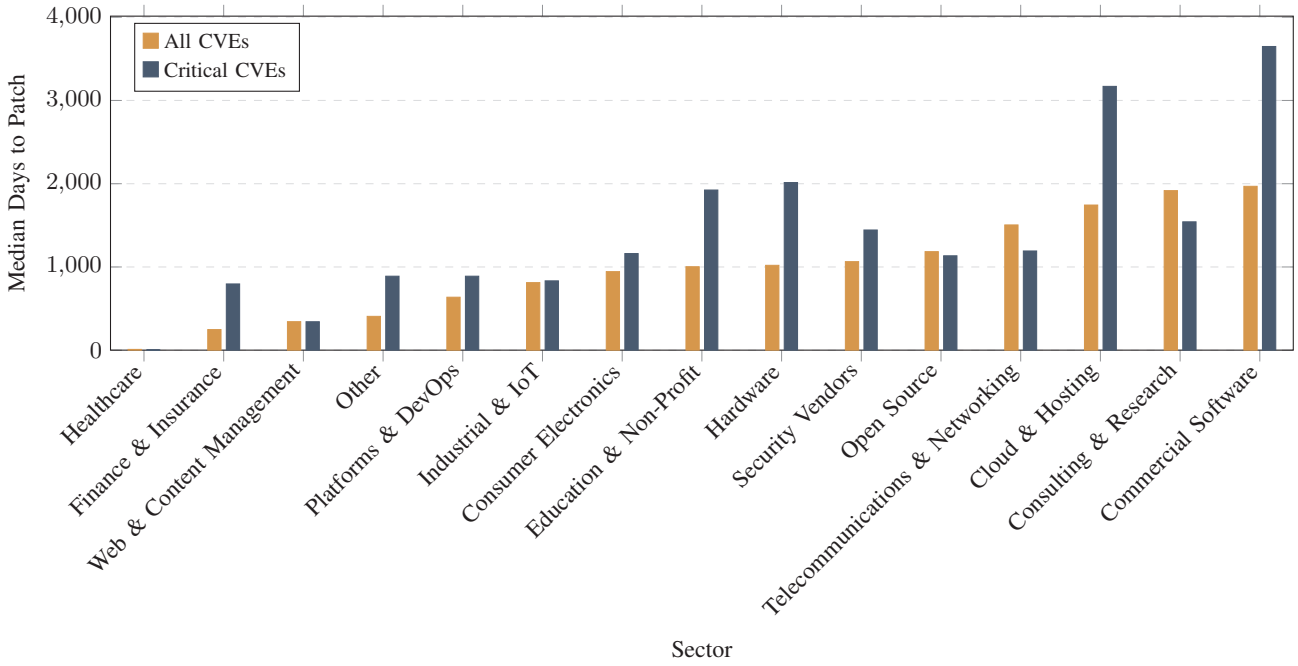

Figure 6. Median time to patch availability by sector (2009 to 2024). Sectors are sorted by overall patch performance (all CVEs). Orange bars represent all CVEs, while blue bars show critical vulnerabilities, revealing significant performance disparities across industries.

A further indication of this is provided by a comparison of performance across different sectors, which shows that open-source communities and cloud providers generally remediate faster than traditional industries, such as commercial software or hardware manufacturing. It is particularly evident in the healthcare, energy, and telecommunications sectors that there is a tendency for shorter patch cycles, which is likely attributable to the presence of more stringent legal and compliance requirements [25][26].

D. Case Study Insights

The quantitative findings are reinforced by qualitative case studies of three landmark critical vulnerabilities (CVSS ≥ 9.0), illustrating real-world manifestation of detection, disclosure, and remediation patterns observed across the 2009-2024 dataset.

The Heartbleed vulnerability (CVE-2014-0160), which was discovered in OpenSSL in April 2014, enabled attackers to read up to 64 KB of server memory, with the potential to expose private keys, passwords and session data for millions of systems worldwide [17]. Despite the rapid provision of patches within two days, the delays between disclosure and remediation in the affected companies averaged more than six months. This was due to widespread dependency on the open-source library and lack of automated detection tools. This case study highlights the challenges associated with the "last mile" of patch deployment, emphasising the necessity for dependency scanning and automated updating within open-source ecosystems to mitigate prolonged exposure windows, which align with the quantitative medians (1,668 days for critical CVEs).

EternalBlue (CVE-2017-0144), which was exploited in the WannaCry ransomware of May 2017, targeted Windows SMBv1 protocol flaws, affecting unpatched Windows systems globally and causing damages in excess of $4 billion [18]. Microsoft released a patch in March 2017 (pre-disclosure), yet six months post-disclosure, 20 % of organisations remained vulnerable, thereby amplifying the subsequent ransomware outbreak. The incident demonstrates the protracted nature of remediation processes in commercial software sectors, extending beyond the established quantitative averages. This emphasises the necessity for regulatory mandates to enforce patch SLAs in critical infrastructures, such as healthcare and telecommunications.

The Log4Shell vulnerability (CVE-2021-44228), which was disclosed in December 2021 in Apache Log4j, enabled remote code execution via malicious logging inputs. This had a significant impact on more than 3 billion devices and triggered immediate zero-day exploits [5]–[7]. Patches were issued within days; however, full remediation took weeks due to supply-chain propagation and configuration complexity, with global adoption lagging as documented in BSI warnings [6]. This finding underscores the existence of persistent organisational delays, thereby signifying the necessity for continuous vulnerability management as opposed to periodic scans, as evidenced by the study's comprehensive patterns.

The collective analysis of these cases serves to reinforce the quantitative patterns identified, thereby illustrating how technical complexity, organisational inertia, and sectoral variations collectively drive the remediation gaps.

V. Discussion And Evaluation

The results of this study highlight both significant progress and persistent structural challenges in the management of critical software vulnerabilities.

Over the period under scrutiny, the time lag between CVE reservation and public disclosure decreased significantly, reaching an average of approximately 33 days in 2024. This phenomenon points to an enhancement in the coordination and responsiveness of the global vulnerability management ecosystem. The expansion of the CNA programme and enhanced collaboration between security researchers, vendors, and vulnerability databases have likely contributed to this acceleration [19][27]. The acceleration of disclosure processes has been demonstrated to increase transparency and enable organisations to initiate defensive measures earlier.

Despite these improvements, the findings demonstrate that faster disclosure does not necessarily lead to faster remediation. The analysis indicates that remediation timelines persistently exceed expectations and demonstrate considerable variability, with a median duration of 1,668 days for critical vulnerabilities. This discrepancy underscores a systemic "last-mile" problem in vulnerability management, where the primary bottleneck shifts from vulnerability discovery to the development and deployment of patches [10].

The existence of this discrepancy can be attributed to a number of factors. In the contemporary context, software systems frequently employ complex dependency chains and interconnected components, a factor that has been shown to complicate the processes of patch development and testing. Moreover, organisational constraints, such as limited resources, operational risks associated with updates, and fragmented asset inventories, have the potential to delay patch deployment, particularly in large or legacy environments.

Sectoral comparisons provide further support for these observations. It is evident that open-source ecosystems and cloud-based platforms frequently demonstrate a higher level of responsiveness, largely attributable to the utilisation of automated development pipelines and continuous integration practices. Conversely, traditional commercial vendors characteristically implement more extended release cycles. It has been demonstrated that regulated sectors, including but not limited to healthcare and telecommunications, exhibit accelerated remediation, a phenomenon that is presumably precipitated by regulatory incentives.

Case studies, including those of Heartbleed, EternalBlue and Log4Shell, illustrate that even when patches are released promptly, organisations frequently require a considerable amount of time to identify affected systems and deploy updates across complex infrastructures. The findings emphasise that effective vulnerability mitigation is contingent not only on vendor response, but also on organisational preparedness and the implementation of mature patch management processes.

The findings indicate an enhancement in vulnerability management with regard to transparency and disclosure efficiency. Nevertheless, the extended remediation timelines underscore a persistent "last-mile" issue in the implementation of patch deployment. In order to address this challenge, it is necessary to implement not only faster vulnerability reporting but also improved automation, better asset visibility, and more mature patch management processes within organisations.

VI. Conclusion and Future Work

The present study examined the processes of detection, disclosure, and remediation of critical vulnerabilities that had severity scores of nine or higher. Integration of data-driven analysis and qualitative case evaluations enabled identification of both structural improvements and persistent challenges in contemporary vulnerability management.

The findings indicate that global disclosure timelines have become considerably reduced, signifying a maturation of the ecosystem of coordinated vulnerability reporting and enhanced cross-organisational communication [24][27]. Nevertheless, the remediation phase continues to demonstrate deficiencies, with notable heterogeneity in patch release times across software vendors and sectors. These delays, frequently attributable to resource constraints, legacy dependencies, and fragmented responsibilities, result in organisations remaining vulnerable for extended periods following the disclosure of vulnerabilities [10].

This work contributes to extant research by quantifying the systemic inefficiencies that persist despite procedural advances. It is also important to note that effective vulnerability management is not just a technical problem, but also a governance challenge [25]. In order to address this challenge, there is a need for synchronised policy, automation and human expertise. Organisations that actively integrate regulatory frameworks, establish prioritised workflows and mandate security accountability are better positioned to reduce the window between discovery and mitigation.

From an applied perspective, this study underscores the necessity for organisations to accord priority to critical vulnerabilities (CVSS ≥ 9.0) through the implementation of established SLAs (cf. Section II) and sector-specific strategies (Subsection IV-C), while concomitantly addressing systemic remediation delays that have been identified across the period 2009 to 2024 (see Figures 4, 5, 6), particularly in commercial software sectors that require a longer timeframe to remediate (cf. Figure 6).

In future research, the exploration of machine learning–driven models, such as exploit prediction scoring systems, in the refinement of prioritisation in dynamic threat environments is recommended. Further investigation into the following areas would be of use in attempting to bridge the gap between awareness and action: automated remediation pipelines; CI/CD-integrated patching; and multi-source vulnerability aggregation [28]. Furthermore, emerging paradigms, such as exposure management and zero-trust architectures offer promising frameworks for the unification of vulnerability management across hybrid infrastructures.

The study indicates that, while the speed of identifying and publishing critical vulnerabilities is improving, sustainable cybersecurity resilience depends on transitioning from reactive

vulnerability management to proactive, continuous exposure governance.

ACKNOWLEDGEMENT

The present paper is founded upon Lena's Master Thesis, which was conducted at the Faculty of Computer Science and Electrical Engineering, Kiel University of Applied Sciences.

REFERENCES

[1] MITRE Corporation, "Frequently asked questions (faqs) - what is cve?", Accessed: 2026-03-14. [Online]. Available: https://www.cve.org/ResourcesSupport/FAQs.

[2] National Institute of Standards and Technology (NIST), "Vulnerability metrics", Accessed: 2026-03-14. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss#.

[3] Ponemon Institute, "Cost of a data breach report 2024", 2024, Accessed: 2026-03-14. [Online]. Available: https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

[4] Bundesamt für Sicherheit in der Informationstechnik, "The state of it security in germany in 2023 (original title in german: Die Lage der IT-Sicherheit in Deutschland 2023)", 2023, Accessed: 2026-03-14. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf.

[5] National Institute of Standards and Technology (NIST), "CVE-2021-44228 detail", Accessed: 2026-03-14. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

[6] Bundesamt für Sicherheit in der Informationstechnik, "Critical vulnerability published in log4j (cve-2021-44228) (original title in german: Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228))", Accessed: 2026-03-14. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=5.

[7] CrowdStrike Intelligence Team, "Log4j2 vulnerability "log4shell" (CVE-2021-44228)", 2021, Accessed: 2026-03-14. [Online]. Available: https://www.crowdstrike.com/en-us/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/.

[8] Forum of Incident Response and Security Teams (FIRST), "Common vulnerability scoring system v4.0 – user guide", Accessed: 2026-03-14. [Online]. Available: https://www.first.org/cvss/v4.0/user-guide.

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI), "OPS.1.1.3: Patch and change management (original title in german: OPS.1.1.3: Patch- und Änderungsmanagement)", 2021, Accessed: 2026-03-14. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.pdf?__blob=publicationFile&v=2.

[10] S. Alexiou, "Practical patch management and mitigation", *ISACA Journal*, vol. 2019, no. 3, pp. 1–6, 2019. Accessed: 2026-03-14. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/practical-patch-management-and-mitigation.

[11] M. Souppaya and K. Scarfone, "Guide to enterprise patch management planning: Preventive maintenance for technology", National Institute of Standards and Technology (NIST), Tech. Rep. NIST SP 800-40 Rev. 4, 2022. Accessed: 2026-03-14. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf4.

[12] J. R. C. Nurse, "To patch or not to patch: Motivations, challenges, and implications for cybersecurity", 2025, Accessed: 2026-03-14. [Online]. Available: https://arxiv.org/pdf/2502.17703.

[13] P. Przymus, M. Fejzer, J. Narębsk and K. Stencel, "The secret life of cves", *arXiv preprint*, 2025. Accessed: 2026-03-14. [Online]. Available: https://arxiv.org/pdf/2504.03863.

[14] P. Przymus, M. Fejzer, J. Narębsk, K. Rykaczewski and K. Stencel, "Out of sight, still at risk: The lifecycle of transitive vulnerabilities in maven", *arXiv preprint*, 2025. Accessed: 2026-03-14. [Online]. Available: https://arxiv.org/pdf/2504.04803.

[15] National Institute of Standards and Technology (NIST), "NVD data feeds - JSON 2.0 feeds", 28th May 2025, Accessed: 2026-03-14. [Online]. Available: https://nvd.nist.gov/vuln/data-feeds.

[16] MITRE Corporation, "CVE list downloads", 20th May 2025, Accessed: 2026-03-14. [Online]. Available: https://www.cve.org/Downloads.

[17] National Institute of Standards and Technology (NIST), "CVE-2014-0160 detail", 2014, Accessed: 2026-03-14. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2014-0160.

[18] National Institute of Standards and Technology (NIST), "CVE-2017-0144 detail", 2017, Accessed: 2026-03-14. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0144.

[19] MITRE Corporation, "CVE numbering authority (cna) operational rules", Accessed: 2026-03-14. [Online]. Available: https://www.cve.org/ResourcesSupport/AllResources/CNARules.

[20] MITRE Corporation, "List of partners", https://www.cve.org/PartnerInformation/ListofPartners, Accessed: 2026-03-14.

[21] MITRE Corporation, "Glossary - cve record", https://www.cve.org/ResourcesSupport/Glossary#glossaryRecord, Accessed: 2026-03-14.

[22] MITRE Corporation, "Process", https://www.cve.org/About/Process, Accessed: 2026-03-14.

[23] National Institute of Standards and Technology (NIST), "CVEs and the NVD process", 2024, Accessed: 2026-03-14. [Online]. Available: https://nvd.nist.gov/general/cve-process.

[24] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Bsi guideline on the coordinated vulnerability disclosure (cvd) process (original title in german: Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess)", 2022, Accessed: 2026-03-14. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf?__blob=publicationFile&v=4.

[25] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Study on the effectiveness of it security laws among operators of critical infrastructures (original title in german: Untersuchung zur Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen)", 2023, Accessed: 2026-03-14. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/evaluierung-itsig2-ergebnisbericht.pdf?__blob=publicationFile&v=3.

[26] World Economic Forum, "Global cybersecurity outlook 2022", 2025, Accessed: 2026-03-14. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[27] MITRE Corporation, "CVE® 25 years - 25th anniversary report october 2024", https://www.cve.org/Resources/Media/Cve25YearsAnniversaryReport.pdf, 2024, Accessed: 2026-03-14.

[28] Forum of Incident Response and Security Teams (FIRST), "Exploit prediction scoring system (epss) - frequently asked questions", Accessed: 2026-03-14. [Online]. Available: https://www.first.org/epss/faq.