NetUSE AG

HAW Kiel
Hochschule für Angewandte Wissenschaften Kiel
Kiel University of Applied Sciences

CVEs With a CVSS Score ≥ 9

Lena Sinterhauf, NetUSE AG in Kiel, Germany
Andreas Aßmuth, University of Applied Sciences in Kiel, Germany
Roland Kaltefleiter, NetUSE AG in Kiel, Germany

20 April 2026 – Lisbon, Portugal

Lena Sinterhauf

- Bachelor’s degree in Information Technology from Kiel University of Applied Sciences
- Master’s degree Information Engineering from Kiel University of Applied Sciences
- Service Delivery Manager at NetUSE AG
- Hands-on experience of IT operations, service delivery and project management
- Focus on optimising processes, coordinating efficiently and ensuring operational resilience in technical environments

Introduction and Motivation

- Critical vulnerabilities (CVSS ≥ 9.0) pose a severe risk to organizations' IT infrastructures.
- Incidents such as Log4Shell, Heartbleed and EternalBlue are notable examples that highlight the urgency and real-world impact of cybersecurity issues.
- Delayed detection or patching can lead to increased financial losses, operational downtime and reputational damage.
- The growing digitisation and interconnectivity of systems widens the attack surface.

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

Research Objectives

Goal: Analyze the speed and efficiency of detecting and resolving critical CVEs (CVSS ≥ 9.0).

Research Questions:

1. How long does it take to detect and disclose critical vulnerabilities?
2. What factors influence the speed of detection?
3. How quickly are critical vulnerabilities remediated in practice?
4. Which technical, organizational and sector-based factors contribute to delays?
5. What improvements can be made to vulnerability and patch management?

Methodology Overview

Mixed-methods Approach

Quantitative analysis:

- 245,456 CVEs (2009–2024)
- ~12.8% critical (CVSS ≥ 9.0)

Qualitative case studies:

- Heartbleed
- EternalBlue
- Log4Shell

Methodology Overview

Mixed-methods Approach

Quantitative analysis:

- 245,456 CVEs (2009–2024)
- ~12.8% critical (CVSS ≥ 9.0)

Qualitative case studies:

- Heartbleed
- EternalBlue
- Log4Shell

Data Sources

- NVD JSON 2.0 feeds
- MITRE CVE database
- Data snapshots: May 2025

Methodology Overview

Mixed-methods Approach

Quantitative analysis:

- 245,456 CVEs (2009–2024)
- ~12.8% critical (CVSS ≥ 9.0)

Qualitative case studies:

- Heartbleed
- EternalBlue
- Log4Shell

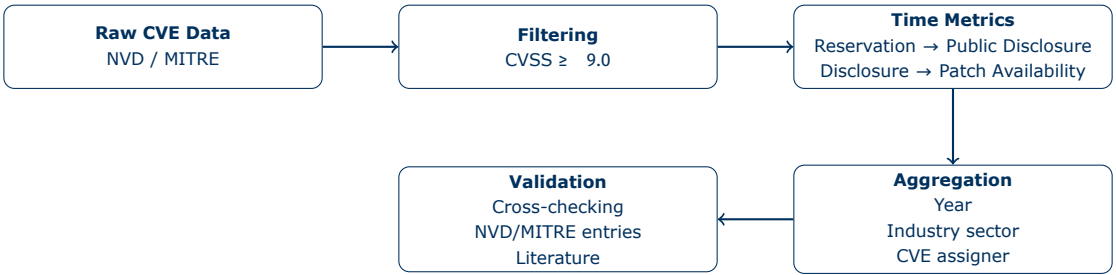
Data Sources

- NVD JSON 2.0 feeds
- MITRE CVE database
- Data snapshots: May 2025

Analysis

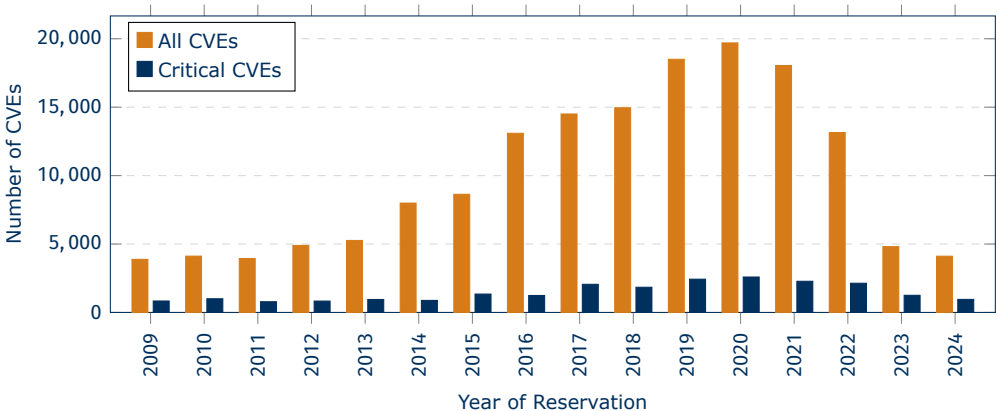
- Reservation → Publication
- Publication → Patch Availability
- Sector-based comparisons

Data Pipeline



Registration and Publication Trends (2009–2024)

Annual distribution of CVE registrations



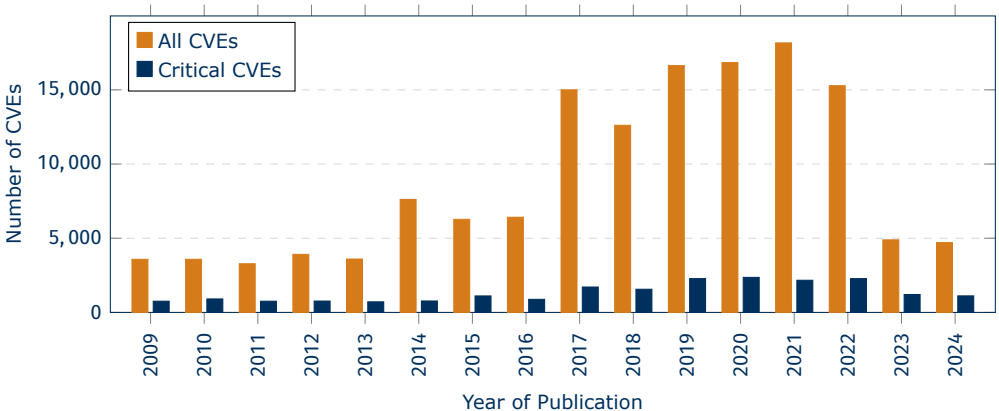
L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

NetUSE AG

HAW Kiel

Registration and Publication Trends (2009–2024)

Annual distribution of CVE publications



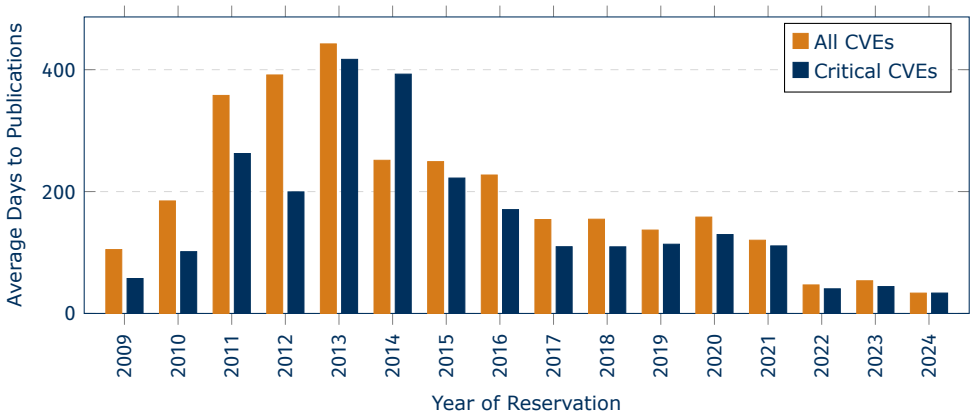
L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

NetUSE AG

HAW Kiel

Time to Disclosure

Average time from CVE reservation to public disclosure



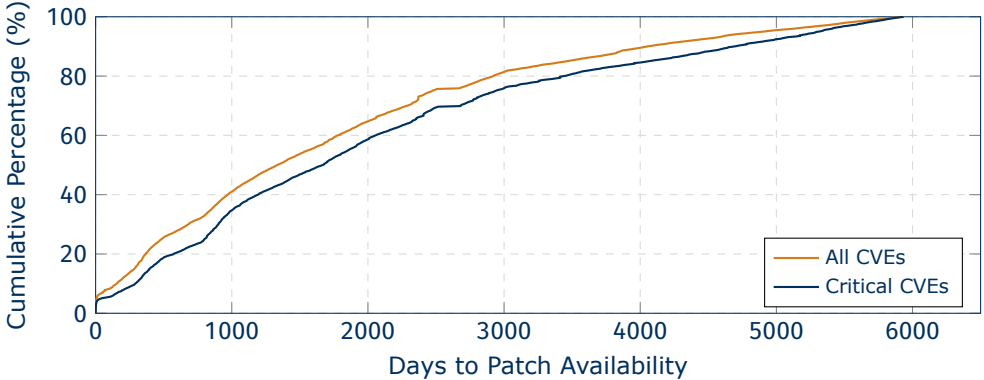
L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

NetUSE AG

HAW Kiel

Patch Availability

Cumulative distribution of time to patch availability

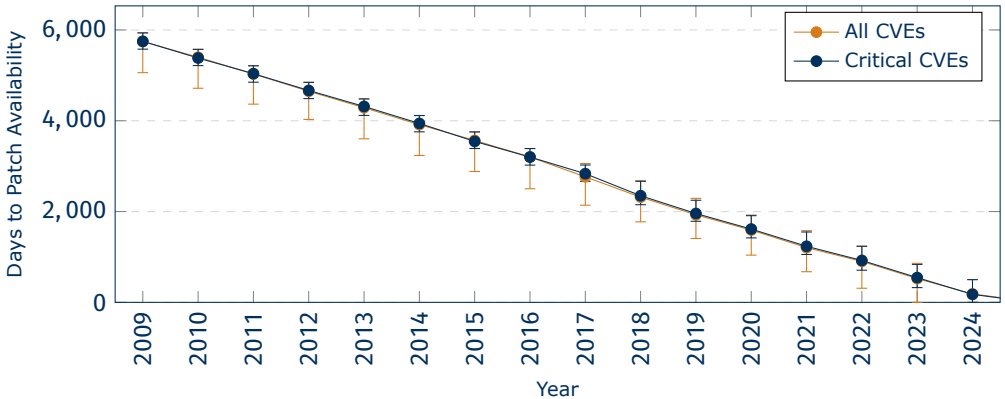


L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

NetUSE AG

HAW Kiel

Patch Availability



L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

NetUSE AG

HAW Kiel

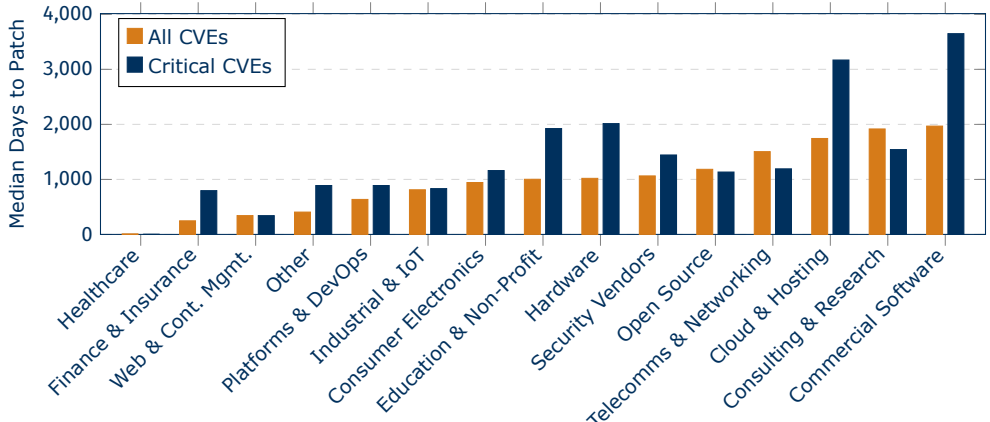
Sector Comparison

Numbers of all and critical CVEs for selected sectors

Sector	All CVEs	Critical
Cloud & Hosting	3,700	263
Commercial Software	41,583	4,658
Consulting & Research	82,386	15,744
Finance & Insurance	66	2
Hardware	13,474	1,276
Healthcare	22	10
Industrial & IoT	2,493	308
Open Source	28,699	2,751
Platforms & DevOps	108	1
Security Vendors	7,249	848
Telecommunication & Networking	13,620	1,476
Web & Content Management	95	25

Sector Comparison

Median time to patch availability by sector (2009 to 2024)



L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

NetUSE AG

HAW Kiel

Case Studies

Heartbleed (CVE-2014-0160)

- The patch was released within 2 days
- The real-world remediation process took months
- The complexity of dependencies caused massive operational delays

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

Case Studies

EternalBlue (CVE-2017-0144)

- The patch existed before it was publicly disclosed (March 2017)
- Months later, > 20% of systems were still vulnerable
- It enabled large-scale attacks (e.g., WannaCry)

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

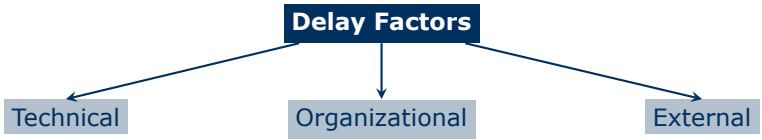
Case Studies

Log4Shell (CVE-2021-44228)

- Exploited within hours of disclosure
- Rapid patch release
- Full mitigation took weeks to months due to the spread of the supply chain

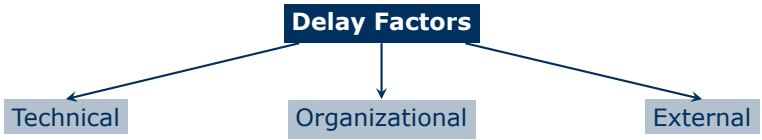
L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

Delay Factors



L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

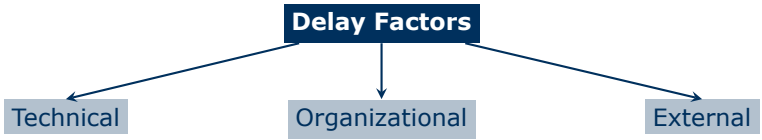
Delay Factors



- Complex software dependencies
- Legacy components
- Lack of automated patching pipelines

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

Delay Factors



- Unclear responsibilities
- Low prioritization
- Missing SOPs
- Insufficient security staffing

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

Delay Factors

- Regulatory / compliance pressures
- Disclosure policy fragmentation
- Vendor-specific release cycles

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

Recommendations

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: “CVEs With a CVSS Score ≥ 9”

NetUSE AG

HAW Kiel

Recommendations

- Increase automation (vulnerability scanning, patch deployment)
- Standardize patch management processes (testing, prioritization)

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

Recommendations

- Create and enforce SOPs
- Improve internal transparency and asset visibility
- Provide continuous security training

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

Recommendations

- Strengthen collaboration (CVD, bug bounty programs)
- Adopt contextual prioritization (CVSS v4.0, EPSS)

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

Conclusion

- There have been major improvements in the speed of disclosure in the vulnerability ecosystem.
- However, remediation remains the major bottleneck, with delays persisting across most sectors.
- Sustainable cybersecurity requires:
  - Automation
  - Governance maturity
  - Cross-organizational collaboration
- Beyond raw CVSS scores, critical CVEs must be prioritized by incorporating context and exploit likelihood.

L. Sinterhauf, A. Aßmuth, R. Kaltefleiter: "CVEs With a CVSS Score ≥ 9"

Q&A

Contact email: lsi@netuse.de