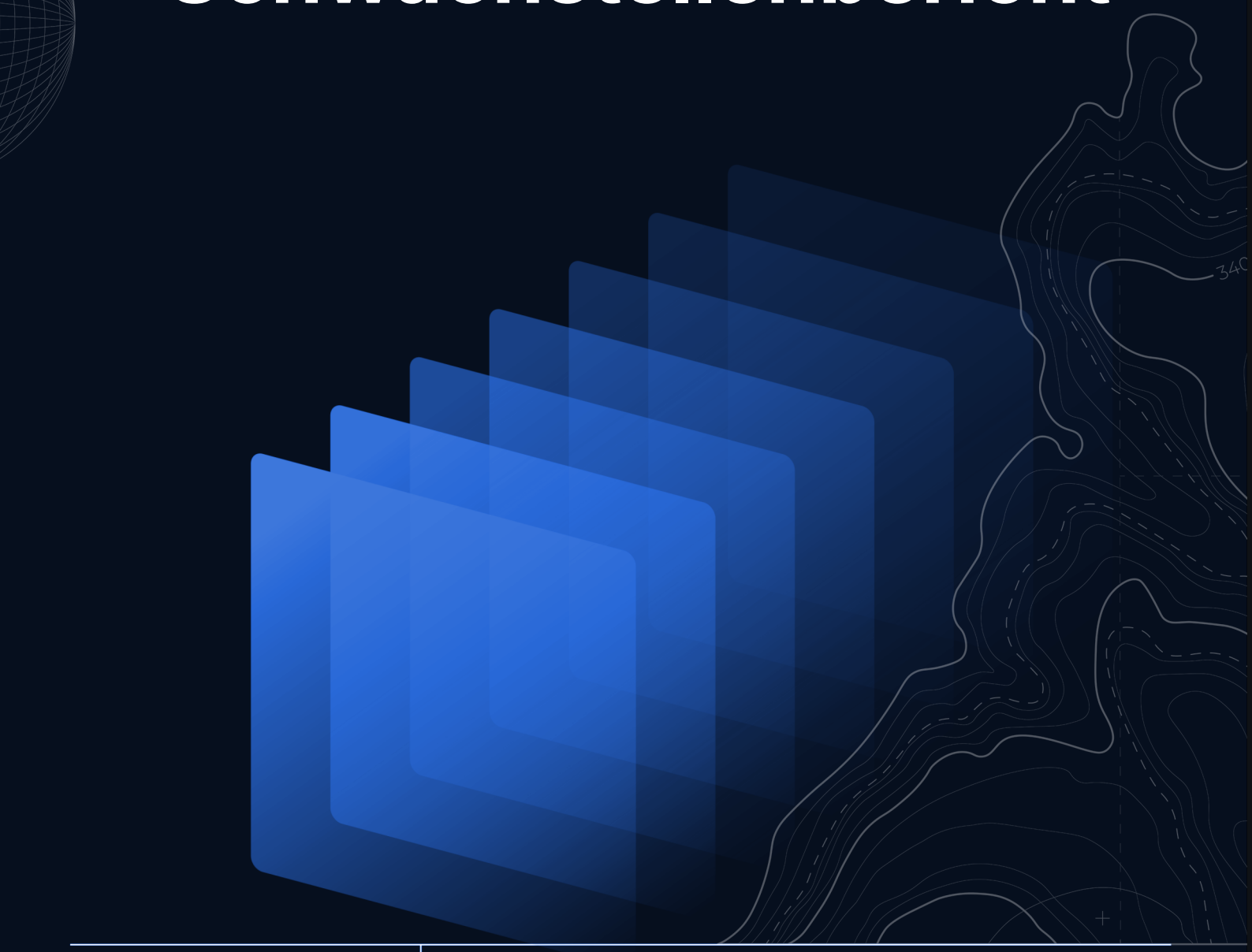
openCode

Schwachstellenbericht



Erstellt für:
ZenDiS GmbH

Datum:
11. June 2025

OPENCODE BADGE API PROJECT

Erzeugt von:
DevGuard

Inhaltsverzeichnis

1 Gegenstand

Dieser Bericht enthält eine Zusammenfassung der bekannten Schwachstellen, die in der Anwendung in Version identifiziert wurden sowie die Einschätzungen dieser Schwachstellen.

- **Anwendung:**
- **Version der Anwendung:**
- **Datum:** 22 August 2025

1.1 Bestandteile

Die Anwendung in Version besteht aus folgenden Komponenten:

- **Komponente 1**
- **Komponente 2**
- **Komponente 3**

2 Zusammenfassung

Die folgenden Grafiken bieten einen Überblick über den aktuellen Stand der Anwendung. Die erste Grafik zeigt die Verteilung der Schwachstellen nach CVSS-Einstufung[1] und verdeutlicht die Anzahl kritischer, hoher, mittlerer und niedriger eingestufter Schwachstellen. Die zweite Grafik stellt die Entwicklung der Schwachstellenanzahl im Verlauf der letzten drei Monate dar und ermöglicht eine Einschätzung des Trends. Die dritte Grafik veranschaulicht die durchschnittliche Behandlungszeit für erkannte Schwachstellen, ebenfalls nach CVSS-Einstufung, und gibt Hinweise auf die Effizienz der ergriffenen Maßnahmen.

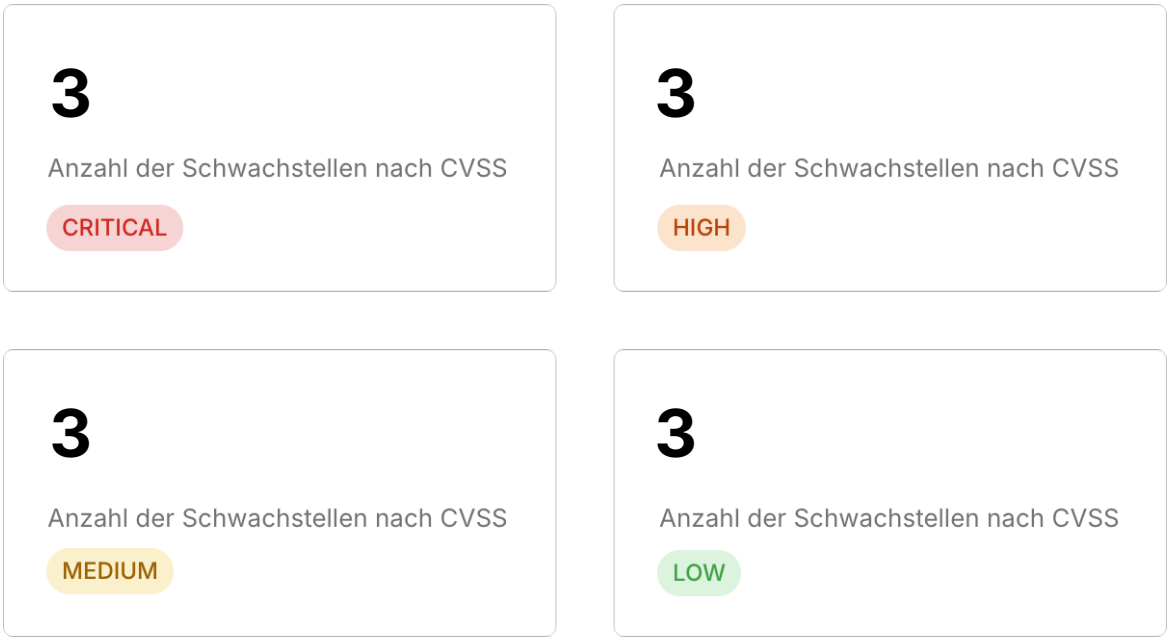


Abbildung 1: Übersicht der Schwachstellen aller Komponente nach CVSS level (3 critical, 3 high, 3 medium, 3 low).

Für die jeweiligen Kritikalitätsstufen sind die folgenden **Behebungszeiten im Mittel** erreicht worden:

- Kritische Schwachstellen: 3 Tage
- Hohe Schwachstellen: 5 Tage
- Mittlere Schwachstellen: 10 Tage
- Niedrige Schwachstellen: 15 Tage

[1] Common Vulnerability Scoring System nach Forum of Incident Response and Security Teams, 2025, verfügbar unter https://www.first.org/cvss/, zuletzt abgerufen am 22. August 2025.

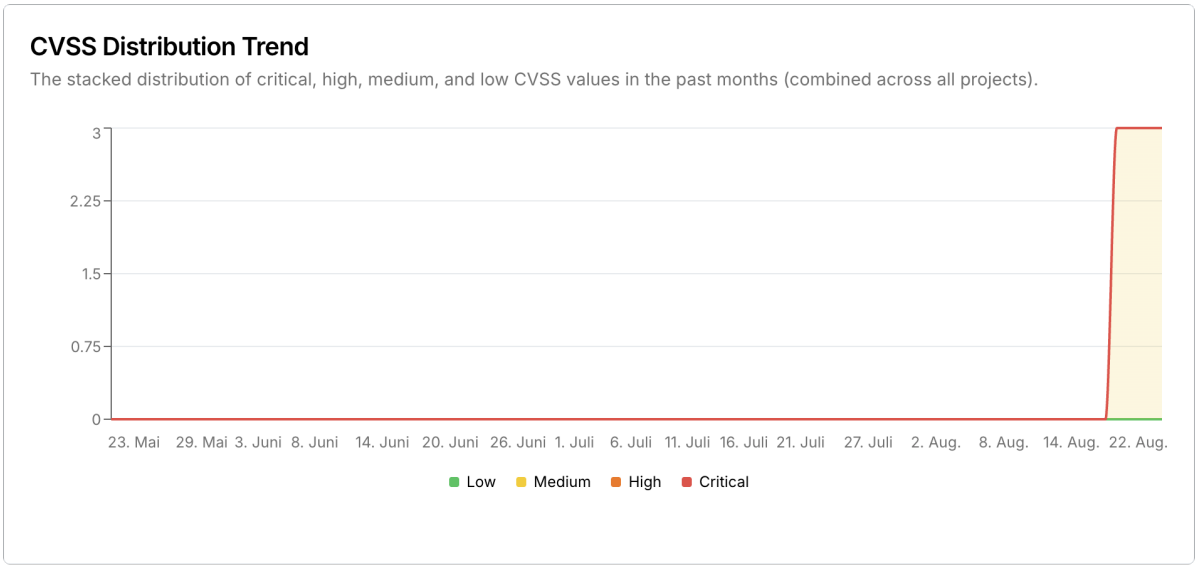


Abbildung 2: Anzahl an Schwachstellen im Verlauf der letzten drei Monate nach CVSS Einstufung

3 Komponente 1 - Version

In diesem Abschnitt werden die bekannten Schwachstellen der Komponente 1 in der Anwendung in Version zusammengefasst. Die Schwachstellen sind nach ihrer CVSS-Einstufung kategorisiert, durch die Einschätzungen des Teams angereichert und geben einen Überblick über die Sicherheitslage dieser Komponente.

3.1 Schwachstellenübersicht

Die folgende Tabelle listet die Anzahl der Schwachstellen nach CVSS-Einstufung für die auf:

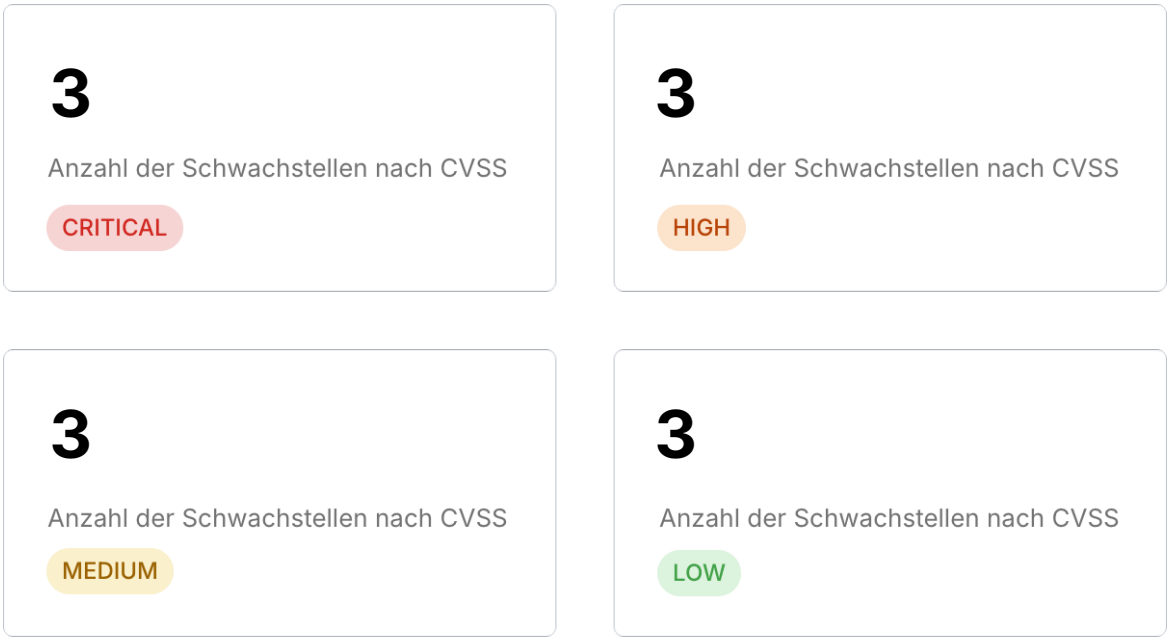


Abbildung 3: Übersicht der Schwachstellen der Komponente nach CVSS level (3 critical, 3 high, 3 medium, 3 low).

Für die jeweiligen Kritikalitätsstufen sind die folgenden **Behebungszeiten im Mittel** erreicht worden:

- Kritische Schwachstellen: 3 Tage
- Hohe Schwachstellen: 5 Tage
- Mittlere Schwachstellen: 10 Tage
- Niedrige Schwachstellen: 15 Tage

3.2 Detaillierte Schwachstellenanalyse

Die nachfolgende Liste enthält die spezifischen Schwachstellen, die in der Komponente 1 identifiziert wurden. Jede Schwachstelle ist mit ihrer CVSS-Einstufung, einer kurzen Beschreibung und den empfohlenen Maßnahmen zur Behebung versehen.

3.2.1 Kritische Schwachstellen

CVE-2014-125026
exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Beschreibung

Helm is a package manager for Charts for Kubernetes. Prior to version 3.18.5, it is possible to craft a JSON Schema file in a manner which could cause Helm to use all available memory and have an out of memory (OOM) termination. This issue has been resolved in Helm 3.18.5. A workaround involves ensuring all Helm charts that are being loaded into Helm do not have any reference of $ref pointing to /dev/zero.

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 9.8 (critical, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

CVE-2014-125026

exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Beschreibung

Helm is a package manager for Charts for Kubernetes. Prior to version 3.18.5, it is possible to craft a JSON Schema file in a manner which could cause Helm to use all available memory and have an out of memory (OOM) termination. This issue has been resolved in Helm 3.18.5. A workaround involves ensuring all Helm charts that are being loaded into Helm do not have any reference of $ref pointing to /dev/zero.

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 9.8 (critical, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

CVE-2014-125026

exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Beschreibung

Helm is a package manager for Charts for Kubernetes. Prior to version 3.18.5, it is possible to craft a JSON Schema file in a manner which could cause Helm to use all available memory and have an out of memory (OOM) termination. This issue has been resolved in Helm 3.18.5. A workaround involves ensuring all Helm charts that are being loaded into Helm do not have any reference of $ref pointing to /dev/zero.

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 9.8 (critical, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

3.2.2 Hohe Schwachstellen

CVE-2014-125026
exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Beschreibung

Helm is a package manager for Charts for Kubernetes. Prior to version 3.18.5, it is possible to craft a JSON Schema file in a manner which could cause Helm to use all available memory and have an out of memory (OOM) termination. This issue has been resolved in Helm 3.18.5. A workaround involves ensuring all Helm charts that are being loaded into Helm do not have any reference of $ref pointing to /dev/zero.

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 7 (high, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

3.2.3 Mittlere Schwachstellen

Es wurden eine mittleren Schwachstellen in dieser Komponente identifiziert.

3.2.4 Niedrige Schwachstellen

Es wurden keine niedrigen Schwachstellen in dieser Komponente identifiziert.

4 Komponente 2 - Version

In diesem Abschnitt werden die bekannten Schwachstellen der Komponente 1 in der Anwendung in Version zusammengefasst. Die Schwachstellen sind nach ihrer CVSS-Einstufung kategorisiert, durch die Einschätzungen des Teams angereichert und geben einen Überblick über die Sicherheitslage dieser Komponente.

4.1 Schwachstellenübersicht

Die folgende Tabelle listet die Anzahl der Schwachstellen nach CVSS-Einstufung für die auf:

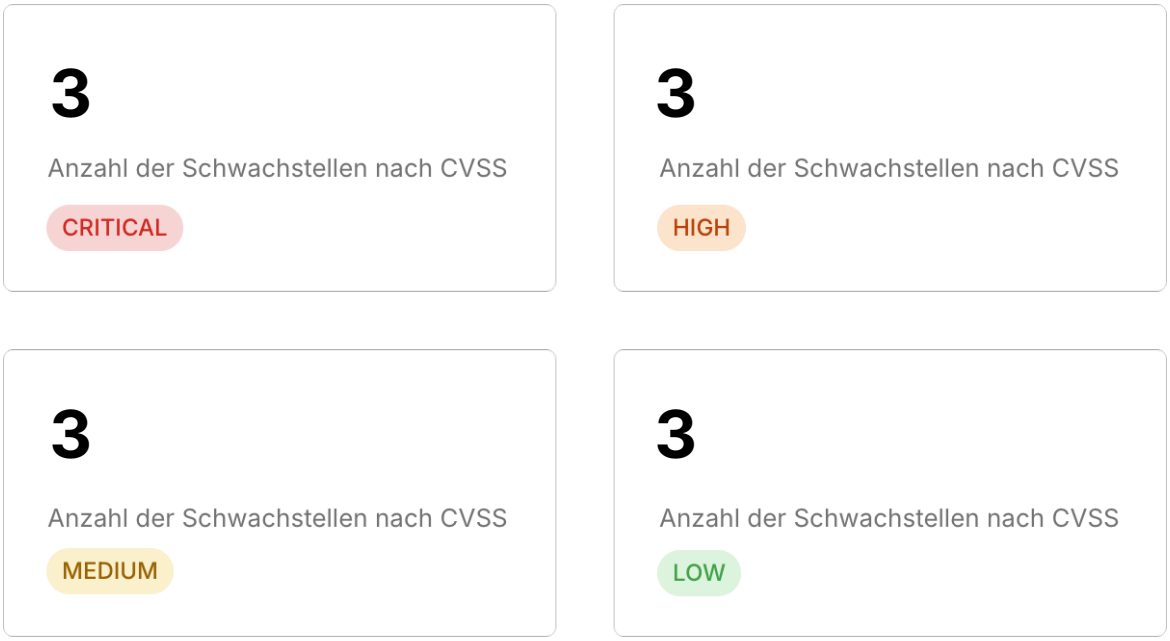


Abbildung 4: Übersicht der Schwachstellen der Komponente nach CVSS level (3 critical, 3 high, 3 medium, 3 low).

Für die jeweiligen Kritikalitätsstufen sind die folgenden **Behebungszeiten im Mittel** erreicht worden:

- Kritische Schwachstellen: 3 Tage
- Hohe Schwachstellen: 5 Tage
- Mittlere Schwachstellen: 10 Tage
- Niedrige Schwachstellen: 15 Tage

4.2 Detaillierte Schwachstellenanalyse

Die nachfolgende Liste enthält die spezifischen Schwachstellen, die in der Komponente 1 identifiziert wurden. Jede Schwachstelle ist mit ihrer CVSS-Einstufung, einer kurzen Beschreibung und den empfohlenen Maßnahmen zur Behebung versehen.

4.2.1 Kritische Schwachstellen

CVE-2014-125026

exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 9.8 (critical, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

CVE-2014-125026

exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 9.8 (critical, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

CVE-2014-125026

exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 9.8 (critical, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

4.2.2 Hohe Schwachstellen

CVE-2014-125026
exploitable, will_not_fix

Referenz

- **ID:** CVE-2014-125026
- **Quelle:** NVD
- **Betroffene Komponente:** pkg:golang/github.com/cloudflare/golz4@v0.0.0-20150217214814-ef862a3cdc58

Analyse

- **Status:** exploitable
- **Reaktion:** will_not_fix
- **Begründung:** We are only using this with trusted input. This is part of the migration SQL-Scripts. The migrations are part of the repository and thus are part of the code review process.
- **Ersteinschätzung:** 01.08.2025
- **Letzte Aktualisierung:** 01.08.2025

Einstufung

- **CVSS Score:** 7 (high, CVSSv3.1)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **DevGuard Bewertung:** 1.5 (low)
- **Vektor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C/CR:H/IR:H/AR:H

4.2.3 Mittlere Schwachstellen

Es wurden eine mittleren Schwachstellen in dieser Komponente identifiziert.

4.2.4 Niedrige Schwachstellen

Es wurden keine niedrigen Schwachstellen in dieser Komponente identifiziert.