
# Fortify.Decidim

Endbericht | Call 18 | Projekt ID 6839

# Inhalt

# 1. Einleitung

Digitale Instrumente kommen bei Partizipationsprojekten immer häufiger zum Einsatz. Open Source Software wie Decidim bietet dabei viele Vorteile (transparenter Code, interinstitutionelle Zusammenarbeit). Damit sensible Daten wie beispielsweise Partei- oder Gewerkschaftsmitgliedschaft bei gezielten Angriffen nicht nach außen dringen können und die Integrität von demokratischen Prozessen nicht kompromittiert wird, wurde im Projekt Fortify.Decidim in Kooperation mit der Pentest-Abteilung des Austrian Institute of Technology (AIT) die Open Source Plattform Decidim einem umfrangreichen Security Audit unterzogen, Schwachstellen repariert und damit die Sicherheit erhöht.

# 2. Projektbeschreibung

Fortify.Decidim machte Decidim widerstandsfähig gegenüber Hackerangriffen, indem in einem automatisierten und manuellen Pentesting (kommerzielle & freie (OS) Schwachstellenscanner sowie statische Code Analyse) High Risk Komponenten identifiziert wurden. Diese High Risk Komponenten wurden manuell vertieft getestet. Damit konnten ein großer Teil der umfangreichen App und zwei Plugins abgedeckt werden.

Den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) folgend wurde der Penetrationstest in folgende fünf Phasen gegliedert:

1. Vorbereitung: In Abstimmung mit dem mitgestalten Partizipationsbüro wurde der Umfang des Penetrationstests festgelegt.
2. Erkundung: Informationen über die Zielsysteme (z.B. Sondierung der Zielhosts auf offene Ports und Identifizierung zugänglicher Dienste) wurden gesammelt.
3. Analyse: Analyse der gesammelten Informationen (d.h. Suche nach bekannten Schwachstellen, Fehlkonfigurationen, Hintertüren, Informationslecks und fehlenden Sicherheitsupdates).
4. Ausbeutung: Überprüfen der identifizierten Schwachstellen durch aktive Ausnutzung.
5. Berichterstattung: Beschreibung der Ergebnisse, Empfehlungen für Abhilfemaßnahmen und Zuweisung von Schweregraden.

Um eine bessere Priorisierung und Konzentration der Abhilfemaßnahmen zu erreichen, wurde jeder Schwachstelle ein numerischer Schweregrad zugewiesen, der auf den technischen Merkmalen der Schwachstelle basiert. Für diese Zuordnung wird das Common Vulnerability Scoring System (CVSS) verwendet. Als Teil dieses Penetrationstests wurde auch eine Codeüberprüfung durchgeführt. Es wurden Sicherheitsrisiken in unterschiedlichen Schweregraden festgestellt.

Diese konnten behoben werden. Sie wurden dem Decidim-Team in Barcelona und den für wichtige Decidim-Module zuständigen Entwicklern über standardisierte Security-Meldungen rückgemeldet.

Das Security Audit bedeutet damit eine Erhöhung der Datensicherheit von bisher 2 Mio. Menschen, die Decidim in Beteiligungsprozessen nutzen. Außerdem unterstützt es sämtliche Decidim-Provider wie: Pokecode, mainiotech, Open Source Politics und das mitgestalten Partizipationsbüro.

Der von der Pentest-Abteilung des Austrian Institute of Technology verfasste Endbericht ist vertraulich und wurde dem Vorstand von netidee sowie den Produktverantwortlichen von Decidim in Barcelona übermittelt. Die Erkenntnisse werden außerdem in einem Online-Call mit den wesentlichen am Decidim-Produkt arbeitenden Entwickler:innen geteilt.

# 3. Verlauf der Arbeitspakete

### 3.1.Arbeitspaket 1 - < Detailplanung und Formales am Projektstart >

Vertrag und Non Disclosure Agreement wurden von netidee und dem mitgestalten Partizipationsbüro unterfertigt.

Projektplanung auf Basis Excel-Vorlage wurde an netidee übermittelt.

Erster Blog wurde erstellt.

Erste Förderrate wurde abgerufen.

### 3.2.Arbeitspaket 2 - < *Kickoff-Meeting und Testumgebung* >

Am 20. Februar 2024 fand das Kick-Off Meeting zwischen mitgestalten Partizipationsbüro, Spread Emotions und dem AIT statt. Dort wurden Scope, Methodik und Zeitplan fixiert. Die Durchführung der Penetrationstests wurde zeitlich geplant. Die Anforderungen an die Testumgebung wurden übermittelt, und Kommunikationskanäle vereinbart.

Alexander Rusa von Spread Emotions setzte daraufhin eine DECIDIM-Testumgebung auf, die von Romy Grasgruber-Kerl vom mitgestalten Partizipationsbüro eingerichtet wurde. Sie ist zu finden auf: https://decidim-audit-org.participation.works/. Besonders aufwändig war es die verschiedenen Benutzerrollen für das AIT einzurichten, sowie jede einzelne Funktion von Decidim in verschiedenen Konfigurationen einzurichten, damit sie getestet werden können. Dieser Arbeitsschritt hat damit mehr Stunden in Anspruch genommen als erwartet.

### 3.3.Arbeitspaket 3 - < *Automatisiertes Testing & manuelles Testing* >

Die Decidim-Applikation und Plugins wurden unter Einsatz führender Schwachstellenscanner und State-of-the-Art Hacking Tools angegriffen. Sämtliche Schwachstellen wurden nach kritischer Bedeutung sortiert und in einem Zwischenbericht zusammengefasst. Die vom AIT erarbeiteten Ergebnisse wurden in einem Koordinationsmeeting am 15. Juli 2024 mit dem mitgestalten Partizipationsbüro und Spread Emotions besprochen und nächste Schritte vereinbart.

### 3.4.Arbeitspaket 4 - < *Vertieftes Automatisiertes Testing & manuelles Testing* >

In einer umfassenden Code-Analys wurden

- Bekannte gefährliche Ruby-Funktionen in Decidim und Decidim Awesome analysiert.
- Vollständige Überprüfung von Decidim Awesome
- Hochriskante Funktionalitäten innerhalb der Anwendung.

Auseinandersetzung mit Rollen und Sichten: Eine detaillierte Analyse der Rollen und Perspektiven innerhalb des Systems, um sicherzustellen, dass die Zugriffsrechte korrekt konfiguriert sind und potenzielle Schwachstellen in der Berechtigungsstruktur aufgedeckt werden.

Überprüfung der GraphQL API: Eine spezifische Prüfung der GraphQL API, um Sicherheitslücken zu identifizieren und sicherzustellen, dass die API-Aufrufe angemessen autorisiert und abgesichert sind. Die Ergebnisse wurden in einem Endbericht zusammengefasst und an den Netidee-Vorstand übermittelt.

### 3.5.Arbeitspaket 5 - < Behebung & Meldung gefundener Sicherheitslücken >

Gefundene Sicherheitslücken wurden bei hohem Schweregrad sofort und bei geringem am Ende des Projekts an die Entwickler von Decidim und Decidim Awesome übermittelt.

Die Förderung durch netidee wird im Patch der durch das Security Audit identifizierte Sicherheitsrisiko angegeben: „This issue was discovered in a security audit organized by the mitgestalten Partizipationsbüro and funded by netidee against Decidim done during April 2024. The security audit was implemented by AIT Austrian Institute of Technology GmbH," (siehe: https://github.com/decidim/decidim/security/advisories/GHSA-7cx8-44pc-xv3q)

Empfehlungen aus dem Endbericht des Security-Audits wurden den Verantwortlichen der Decidim-Plugins Decidim Awesome mitgegeben.

Die Empfehlungen des AIT wurden von Spread Emotions in einer eigens angelegten Testumgebung erneut geprüft. Jene relevanten Risiken, die am Projektende noch nicht vom Decidim Team behoben wurden, wurden von Spread Emotions geschlossen und per Pull Request übermittelt. Da der Schweregrad sehr gering ist, wurde auf das Einbringen über die offizielle Security-Policy-Seite verzichtet.

Laut Security Policy von Decidim werden Sicherheitslücken erst 2-4 Monate nach Behebung veröffentlicht, um Decidim-Providern Zeit zum Aktualisieren zu geben.

### 3.6.Arbeitspaket 6 - < Dokumentation und Formales am Projektende >

Die geplanten Projektergebnisse (siehe Arbeitsblatt "Projektergebnisse") sind erstellt/ funktionsfähig und ausreichend dokumentiert.

Projekt-Website wurde ein letztes Mal aktualisiert: Projektergebnisse sind unter Angabe der open source bzw. creative commons Lizenz der Öffentlichkeit zur Verfügung gestellt,

Projektendbericht und Endabrechnung sind abgenommen; abschließender Projektblogeintrag; letzte Förderrate beantragt.

# 4. Umsetzung Förderauflagen

Für das Projekt wurde ein Non Disclosure Agreement zwischen dem netidee-Vorstand und dem mitgestalten Partizipationsbüro abgeschlossen. **Davon ist das wichtigste Projektergebnis, nämlich der durch das AIT erstellte Report über das Security-Audit betroffen. Dieser wurde dem netidee-Vorstand übermittelt, kann jedoch nicht der Öffentlichkeit zugänglich gemacht werden.**

# 5. Liste Projektendergebnisse

| | | | |
|---|---|---|---|
| ~~*1*~~ | ~~*Projektzwischenbericht*~~ | ~~*CC BY 4.0 oder CC BY SA 4.0*~~ | ~~*netidee.at/Projektseite*~~ |
| *2* | *Projektendbericht* | *CC BY-SA 4.0* | *https://www.netidee.at/fortifydecidim* |
| *3* | *Entwickler_innen-DOKUMENTATION des Projektergebnisses für andere Entwickler_innen ("Dritte"), die das Projektergebnis nach Projektende nutzen/ weiterentwickeln wollen.* | *AGPL 3.0* | *https://github.com/decidim/decidim/security*<br>*https://github.com/decidim/decidim/pulls*<br>*https://github.com/decidim-ice/decidim-module-decidim_awesome/pulls* |
| *4* | *Anwender_innen-DOKUMENTATION des Projektergebnisses für Anwender_innen, die das Projektergebnis nach Projektende nutzen wollen* | *CC BY-SA 4.0* | *https://www.netidee.at/fortifydecidim* |

| | | | |
|---|---|---|---|
| *5* | *Veröffentlichungsfähiger Einseiter / Zusammenfassung* | *CC BY-SA 4.0* | *https://www.netidee.at/fortifydecidim* |
| *6* | *Dokumentation Externkommunikation zur Erreichung Sichtbarkeit /Nachhaltigkeit (Teil des Endberichtes)* | *CC BY-SA 4.0* | *https://www.netidee.at/fortifydecidim* |
| *7* | *Dokumentation: Phase 1*<br>*Öffentlich einsehbar: Bereitstellung Test-Umgebung: Die neueste Decidim 0.28 Umgebung wird als Testumgebung eingerichtet.*<br>*Vertraulich: Als Teil von Zwischenbericht/ Konzept* | *Confidential*<br>*AGPL 3.0* | *https://decidim-audit-org.participation.works/* |
| *8* | *Konzept für zweite Testphase* | *Confidential* | |
| *9* | *Abschlussbericht über gefundene Sicherheitsrisiken* | *Confidential* | |
| *10* | *Code-Verbesserungen: Behebung identifizierter Sicherheitslücken im Code* | *AGPL 3.0* | *https://github.com/decidim/decidim/security*<br>*https://github.com/decidim/decidim/pulls*<br>*https://github.com/decidim-ice/decidim-module-decidim_awesome/pulls* |
| *11* | *Verschlüsselte Meldung: Verantwortungsvolle Meldung weiterer offener Sicherheitslücken.* | *Confidential* | |

# 6. Verwertung der Projektergebnisse in der Praxis

Die im Projekt gefundenen Schwachstellen wurden repariert. Die daraus entstandenen Security-Patches fließen automatisch in jedes weitere Update von Decidim ein, und kommen damit allen Decidim-Anwender:innen zu Gute.

Das mitgestalten Partizipationsbüro organisiert einen Online-Call, wo der Bericht und die Empfehlung von Alexander Rusa den federführenden Developer:innen der Decidim-Community vorgestellt werden.

## 7. Öffentlichkeitsarbeit/ Vernetzung

Externkommunikation erfolgte zu Projektbeginn und am Projektende über LinkedIn-Posts und auf auf der Website von netidee und über die Website des mitgestalten Partizipationsbüro: https://partizipationsbuero.at/fortify-decidim/

Das Projekt wurde außerdem bei allen 2024 erfolgten Teilnahmen des mitgestalten Partizipationsbüro an öffentlichen Ausschreibungen angeführt.

Der Fokus des Projekts lag allerdings weniger auf der externen, sondern auf Vernetzung und der internen Kommunikation innerhalb der internationalen Decidim-Community. Für die Zielgruppe der Developer:innen-Community werden Projekt und Fördergeber durch die namentliche Nennung in Security-Patches bekannt gemacht, außerdem wurden Projekt und Fördergeber in sämtlichen Kommunikationen (E-Mails, Online-Calls) namentlich angeführt. Vernetzung zwischen der AIT Pentesting-Abteilung und den Produktverantwortlichen von Decidim und Decidim-Awesome fanden statt. Diese Kontakte könnten in Zukunft der Sicherheit von Decidim zuträglich sein.

In einem Online-Call mit den führenden Decidim-Developer:innen wurden die Ergebnisse präsentiert. Alexander Rusa arbeitet nun am Decidim Security Advisory mit. Die Reaktionsschnelle und Professionalität der Entwickler von Decidim und Decidim Awesome wurden vom AIT besonders gelobt, d.h. es gab hier ein genuines Interesse, das nicht eingefordert werden musste.

## 8. Eigene Projektwebsite

*Keine*

## 9. Geplante Aktivitäten nach netidee-Projektende

Die langfristige Wirkung des Projekts ist mit jeder neuen und weiterhin aktiven Decidim-Plattform sichergestellt, da die Projektergebnisse in die Open Source Software einfließen.

## 10. Anregungen für Weiterentwicklungen durch Dritte

Im Rahmen des Security-Audits erarbeitete Empfehlungen wurden den Produktverantwortlichen der Decidim-Plattform sowie des Plugins Decidim Awesome vertraulich übermittelt.