

Contao-Support

Contao ist ein Open Source-Projekt, getragen von einer gemeinnützigen Community, die kostenfreien Support im Forum leistet. Neben diesem Community-Support gibt es eine kommerzielle Alternative für professionelle Nutzer, die von den Contao-Partnern angeboten wird.

Die Partner betreuen bei Bedarf auch Deine Webseite, erstellen individuelle Erweiterungen oder bieten Contao-Hosting.



Häufig gefragt

Die am häufigsten
gestellten Fragen
durchsuchen

[FAQs ansehen](#) >



News

Die offiziellen
Ankündigungen zu
Contao lesen

[News lesen](#) >



Benutzerhandbuch

Das Contao-Handbuch
für Benutzer lesen

[Benutzerhandbuch](#) >



Contao-Partner

Finde einen Contao-
Partner in Deiner Nähe

[Contao-Partner](#) >



Community-Support

Kostenloser Support von
und für Contao-Nutzer

[Contao Forum](#) >



Slack

Offizieller Slack-
Workspace für Contao

[Slack-Workspace](#) >



Bücher & Videos

Contao-Bücher, Videos
und andere
Publikationen

[Bücher & Videos](#) >



Entwicklerhandbuch

Das Contao-Handbuch
für Entwickler lesen

[Entwicklerhandbuch](#) >

Sicherheitshinweise

Hier findest du eine Übersicht der Sicherheitslücken, die in Contao bereits gefunden und behoben wurden.

SQL-Injection im Dateimanager

Datum: 30.04.2019

CVE-ID: CVE-2019-11512

Die Suchfunktion des Dateimanagers ist anfällig für SQL-Injections. Das Problem betrifft alle Contao-Versionen ab Contao 4.1 und wurde in Contao 4.4.39 und 4.7.5 behoben.

[Weiterlesen ...](#) 

Invalidierung von Opt-In-Tokens

Datum: 09.04.2019

CVE-ID: CVE-2019-10643

Bei der Bestätigung eines Opt-In-Tokens werden vorherige Opt-In-Tokens nicht invalidiert. Das Problem betrifft Contao 4.7 und wurde in Contao 4.7.3 behoben.

[Weiterlesen ...](#) 

Umgehung der Request-Token-Prüfung

Datum: 09.04.2019

CVE-ID: CVE-2019-10642

Archiv


 [2019 – 4 Einträge](#)

 [2018 – 3 Einträge](#)

 [2017 – 2 Einträge](#)

 [2015 – 2 Einträge](#)

Sicherheitsrichtlinie

Wenn du glaubst ein Sicherheitsproblem in Contao gefunden zu haben, melde es bitte gemäß unserer  [Sicherheitsrichtlinie](#).