re Datenschutz-Einstellungen

personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

Weitere Informationen finden Sie im Cookie-Hinweis.

Cookie-Einstellungen

Nur erforderliche Cookies setzen

Alle Cookies akzeptieren

Article

Marmind Authorization Bypass

An Authorization Bypass vulnerability in the Marmind web application with version 4.1.141.0 allows users with lower privileges to gain control to files uploaded by administrative users. The accessed files were not visible by the low privileged users in the web GUI. The vulnerability was reported as CVE-2020-26506.

Background

We discovered a security issue within the Marmind web application with version 4.1.141.0. It is a software that combines campaigns, budgets and results into one central marketing plan. An attacker that has access to the network or a disgruntled employee can access files, which should not be available to the assigned roles that they have.

Steps to Reproduce

Upon creating a new campaign, an administrative user is able to upload new files in the part "Assets" of the web application. Users with adequate permissions could download all the existing assets from a specific campaign. After successful navigation to the URL of the asset from the campaign that is targeted, the user without privileges gets a HTTP response that the access to the asset has been denied. However, even though the user is not authorized to access the asset, a successful download has been automatically started and the file has been downloaded to the computer of the user.

The following pictures show how we are able to exploit the vulnerability:

Root Cause

This issue exists due to broken access controls of the web application. In order to mitigate the issue, we recommend that the server should verify whether the given user has the necessary privileges before performing any actions. The verification should be done with the help of the server side session (identified by the session token sent by the client).

Fix/ Producer Statement

The issue was reported to Marmind. The identified business threat was evaluated and a fix has been implemented.

In the current version 4.1.146.0, general changes have been made in providing binary data through the API of Marmind. In the previous versions of Marmind, the binaries were directly accessed over a reverse proxy hosted in the dedicated Media Asset Management Service, which has no user authorization functionalities. The direct routes to the Media Asset Management Service are now removed and a new API gateway has been implemented that ensures proper authorization checks upon a request to a specific application's asset.

Credit

Credit for finding and reporting the issue:
• Evgeni Sabev (Deloitte)

Your Contact

Christian Duewel
Director | Cyber Defense & Managed Security Services
cduewel@deloitte.de | +49 40 320804138

Christian ist Director im Bereich Cyber Defense und Managed Security Service mit mehr als 20 Jahren umfassender praktischer Erfahrung im Bereich Cybersicherheit. Sein Fokus liegt auf der Entwicklung u... Mehr

Auch interessant

https://www.facebook.com/Deloitte.Deutschland

https://twitter.com/DeloitteDE

https://www.linkedin.com/company/deloitte/

https://www.xing.com/company/deloitte

https://www.instagram.com/deloittedeutschland/karriere/

http://www.youtube.com/user/DeloitteDeutschland

Deloitte.

Ihre Datenschutz-Einstellungen

Deloitte setzt Cookies ein, um die einwandfreie Funktion unserer Webseite zu gewährleisten, statistische Analysen zur Optimierung unserer Webseite durchzuführen und zusammen mit Drittanbietern Inhalte und Werbung zu personalisieren.

Wenn Sie auf **"Alle Cookies akzeptieren"** klicken, stimmen Sie der Platzierung dieser Cookies auf Ihrem Gerät zu. Sie können diese Cookies jederzeit ablehnen oder verwalten, indem Sie auf **"Cookie-Einstellungen"** klicken. Je nach den von Ihnen gewählten Cookie-Präferenzen kann es sein, dass die volle Funktionalität oder das personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

Weitere Informationen finden Sie im Cookie-Hinweis.

© 2022. See Terms of Use for more information.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/about to learn more about our global network of member firms.