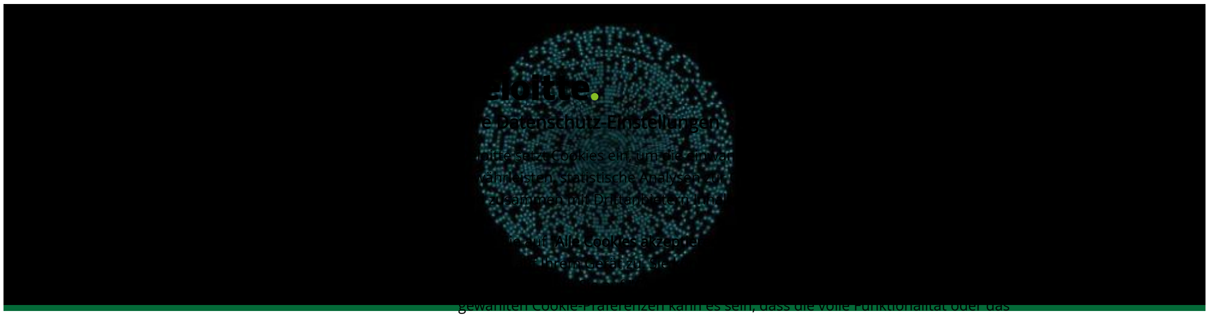

gewählten Cookie-Präferenzen kann es sein, dass die volle Funktionalität oder das personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

Weitere Informationen finden Sie im Cookie-Hinweis.

Cookie-Einstellungen

Nur erforderliche Cookies setzen

Alle Cookies akzeptieren

Article

Marmind XSS

A Stored Cross-Site Scripting (XSS) vulnerability in the “Marmind” web application with version 4.1.141.0 allows an attacker to inject code that will later be executed by legitimate users when they open the assets containing the JavaScript code. This would allow an attacker to perform unauthorized actions in the application on behalf of legitimate users or spread malware via the application. By using the “Assets Upload” function, an attacker can abuse the upload function to upload a malicious PDF file containing a stored XSS. The vulnerability was reported as CVE-2020-26505.

Background

We discovered a security issue in the „Marmind” web application. It is possible to inject JavaScript code within the “Assets Upload” function of the product due to a lack of sufficient input filtering. An attacker can inject malicious file containing JavaScript code that will later be executed by legitimate users who open the malicious files. An attacker may perform unauthorized actions on behalf of legitimate users or spread malware via the application. Additionally if a user opens the PDF, their PDF renderer could send a request to the attacker, revealing their IP address, and by extension, their location.

Steps to Reproduce

The application performs limited filtering of XSS. However by using PDF with embedded JavaScript code in it, we were able to bypass it. The filtering is based on a blacklist approach and not all payloads are recognized. We used the build-in app.alert() function for JavaScript in PDFs to circumvent the protection. This results in a successful Stored XSS. The following pictures show how we were able to exploit the vulnerability.

Root Cause

This issue exists due to insufficient input filtering of the files uploaded by the “Assets Upload” function. In order to mitigate the issue, we recommend applying input filtering to all uploaded files in the entire application to ensure that only valid content is processed (this means input filtering for the fields as well as for the field values). We also recommend ensuring the library used for rendering is robust, as it will be parsing potentially malicious content on the server side. Additionally, setting up a sandboxed environment could further help to reduce the attack surface.

Fix/ Producer Statement

The issue was reported to Marmind. The identified business threat was evaluated and does not pose a high security threat to the Marmind users.

The Chrome PDF-preview viewer is sandboxed and most of the browsers block the execution of JavaScript code in a PDF-preview mode. The PDF itself only supports a specific set of JavaScript code that can be embedded as the one used in the example above.

The PDF specifications at http://partners.adobe.com/public/developer/en/acrobat/sdk/5186AcroJS.pdf lays out that the set of JavaScript objects, where PDFium supports a subset of those objects. PDFium stubs out the dangerous objects and methods listed in the above PDF specifications by Adobe where only triggering the alert() function is still permitted because it should not pose a threat to the end users. Through the XSS vulnerability, no cookies or other private data were extracted.

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
in

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

Home
Über Deloitte Deutschland

Deloitte-Stiftung

Alumni

Events

Pressemitteilungen

Blogs

Podcasts

Angebotsanfrage

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/deloittedeutschlandkarriere/

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.

Services

Audit & Assurance

Risk Advisory

Tax

Legal

Financial Advisory

Consulting

Deloitte Private (Mittelstand)

Spotlight

Industries

Consumer

Energy, Resources & Industrials

Financial Services

Government & Public Services

Life Sciences & Health Care

Technology, Media & Telecommunications

Careers

Jobsuche

Berufserfahrene

Studierende

Karriere bei Deloitte

Schüler:innen

Absolvent:innen

Über Deloitte | Rechtliche Hinweise | Cookies | Impressum | Datenschutzhinweise

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.