

personalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.

Article

Weitere Informationen finden Sie im Cookie-Hinweis.

Marmind CSV Injection

A CSV Injection (also known as Formula Injection) vulnerability in the Marmind web application with version 4.1 141.0 allows malicious users to gain remote control of other computers. By providing formula code in the "Notes" functionality in the main screen, an attacker can inject a payload into the "Description" field under the "Insert "To-Do" option. Other users might download this data, for example a CSV file, and execute the malicious commands on their computer by opening the file using a software such as Microsoft Excel. The attacker could gain remote access to the user's PC. The vulnerability was reported as CVE-2020-26507. Alle Cookies akzeptieren

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 can embed malicious commands within the formula data of a spreadsheet due to a tack of sufficient input filtering. This may lead users to become compromised should they open the injected spreadsheet that was exported as a CSV file opened via tools like Microsoft Excel or LibreOffice. The attacker can infect users with malware and gain control over their machine, if the malicious code is executed successfully.

Steps to Reproduce

Upon creating a new to-do task, a malicious user is able to enter formula code into the "Description" field. Users with adequate permissions, could export and download all the existing companies in the database as a CSV flie. If the infected CSV flie is opened with Microsoft Excel the malicious formula code will be executed, after the user accepts the warring from the popup window in Excel that the program "rnd. exe!" will be executed upon opening the document. Because the file comes from a trusted source and because of the click-through habit of users, we assume that the warning message would be ineffective.

In this example, the value "=c md | "/C calc"!A0" was used as description for the to-do task. The formula is then interpreted by Excel and the embedded commands are executed.

Root Cause

This issue exists due to insufficient input filtering. In order to mitigate the issue, we recommend sanitizing cells that begin with any special character that may trigger the execution of a formula such as "=", "+", "@" or ".". By prepending a single quote or apostrophe () character to the field's content may avoid the content of the cell from being interpreted as a formula.

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.

After exporting a potentially malicious report in XLSX format and opening the file on a user-device, a user gets a warning message and the execution of such formula codes is blocked by default.

Marmind consider input validation not needed for the identified special characters that would only be a threat in specific output formats. Marmind uses Microsoft Reporting Services to render and export the XLSX and CSV files in which exists no native sanitizing.

Credit

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

Your Contact



Murat Yildiz

Partner | Cyber

myildiz@deloitte.de +49 6211590125



Murat Yildiz führt das lokale Cyber Intelligence Center Team in Deutschland, wobei er sich mit Themen wie SOC / SIEM, Threat Intelligence, Penetration Testing, Source Code Review usw. beschäftigt.

Auch interessant

Iobsuche Kontakt Angebotsanfrage Newsletter | | | |



			Uber Deloit
Home			
Über Deld	pitte Deutschland		
Deloitte-9	itiftung	Deloitte.	
Alumni			
Events		Ihre Datenschutz-Einstellungen	
Pressemitteilungen		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.	
Blogs			
Podcasts		Wenn Sie auf "Alle Cookies akzeptieren" klicken, stimmen Sie der Platzierung dieser	
Angebotsanfrage		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	
f	https://www.facebook.com/Deloitte.L	Deutsenssenalisierte Nutzererlebnis dieser Website nicht zur Verfügung stehen.	
y	https://twitter.com/DeloitteDE	Weitere Informationen finden Sie im Cookie-Hinweis.	
in	https://www.linkedin.com/company/d		
×	https://www.xing.com/company/deloitte		
https://www.instagram.com/deloitted		leutschlandkarriere/	
0	http://www.youtube.com/user/Deloitt	teDeutschland	
Sei	rvices		
Audit & Assurance Risk Advisory			
Tax	Advisory		
Lega	al		
Financial Advisory			
	sulting		
Deloitte Private (Mittelstand) Spotlight			
Inc	lustries		
Con	sumer		
	rgy, Resources & Industrials		
Financial Services			
Gov	Government & Public Services		
Life	Sciences & Health Care		
Tech	nnology, Media & Telecommunications		
Ca	reers		
lohs	uche		

© 2022. See Terms of Use for more information.

Berufserfahrene Studierende Karriere bei Deloitte Schüler:innen Absolvent:innen

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.