Article

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.

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 lack of sufficient input filtering. This may lead users to become compromised should they open the injected spreadsheet that was exported as a CSV file and 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 file. If the infected CSV file is opened with Microsoft Excel the malicious formula code will be executed, after the user accepts the warning from the popup window in Excel that the program "cmd .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. Her... 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

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