SECURITY CHANGES AND ENHANCEMENTS IN FILEMAKER® PRO 2024 (V-21)

By:

Wim Decorte

and

Steven H. Blackwell

Claris Platinum Members are independent entities without authority to bind Claris International, Inc. and Claris International, Inc. is not responsible or liable for their actions.

The views and recommendations expressed in this White Paper are solely those of the authors and may not necessarily reflect those of Claris International, Inc.
FileMaker Pro® and FileMaker® Server are registered trademarks of Claris International, Inc. of Sunnyvale, California.

Version 1.2

Since the launch of FileMaker® Pro 7 over twenty years ago, there has been an on-going effort by Claris/FileMaker and by some members of the Developer Community to improve the Security features of the Family of Products, including correcting vulnerabilities and adding enhancements.

Some examples of these activities include the following:

•The introduction of the *fmextscriptaccess* Privilege Bit to provide positive control over the use of Apple Events and ActiveX for performing actions on the Data, Metadata, Schema, and Business Logic of FileMaker files.[1]

•The introduction of the *fmurlscript* Privilege Bit to provide positive control over the use of the FMPURL functionality.

•The introduction of the *File Access Protection* feature to enhance control over use of external methods of access and control of Data, Metadata, Schema, and Business Logic of FileMaker files.

•The introduction of *Encryption At Rest* (EAR) to protect the binary files created by FileMaker Pro.

All of these features had as a central and underlying purpose making files ***Secure By Default***. This means that the default setting, whether *On* or *Off*, was to be the most secure setting option.

The authors have been centrally involved in the adoption of these enhancements. And it is from that perspective and with that background that we come to this White Paper.

—WHY DO WE HAVE SECURITY FEATURES?—

The core purpose of Security is to assure the ***Confidentiality, Integrity, Availability, and Resilience*** of FileMaker Pro solutions.

Confidentiality, as the name suggests, is directed at providing that only those persons authorized to have access to the data and to the system are allowed to do so.

Integrity refers to protecting the results that the Business Processes provided by the system deliver so that users can be assured that data have not been subject to unauthorized alternation or tampering, sometimes of a very subtle and undetectable nature.

Availability, as the name suggests, refers to protecting the physical existence and accessibility of the system and protecting it against attack or accidents.

---

[1] https://fmforums.com/blogs/entry/1738-behavior-change-api-privileges-in-version-16/

Finally, *Resilience* (a comparatively new concept) refers to the ability to restore the data or the system from damage, accidents, or other mishaps. *The entire FileMaker Platform Security Schema is directed at supporting and providing these four elements.*

It is of particular and significant importance that Developers employ all the available Security options correctly in order to imbue the FileMaker Pro files with the most widespread and effective Security the Platform can offer. This is particularly true for *File Access Protection*, *fmextscriptaccess, fmurlscript* , and *Encryption At Rest* (EAR) as noted above. These elements work together in concert to protect the FileMaker Pro file.

—THE NEW VERSION—

The recent release of FileMaker® Pro 21 (aka FileMaker® Pro 2024) continues these efforts. In this White Paper we will discuss most of the Security information relevant to this new release as well as some aspects of other recent patches issued by Claris.

Much of the specific discussion herein focuses on *items within the purview and control of the developer*, rather than of Claris, and **thus it warrants more attention.** We will reference some of those other Security items later in the Paper so that members of the Developer Community can be aware of them and monitor their respective installation and usage of the Family of Products.

SPECIFIC VULNERABILITIES ADDRESSED IN NEW VERSION

There are two specific Security vulnerabilities that have been addressed and corrected in FileMaker Pro 21. We will review each in turn, describe it, describe how it could be triggered, and describe the remediation of it.

UNEXPECTED ACCESS TO DATABASE SCHEMA

The first vulnerability was that a *Subordinate Level*[2] *User* of a system could gain access to Database Schema and then make changes, including additions, deletions, and modifications to Schema elements:

[2] A *Subordinate Level User* is one whose designated Privileges do not include access to the Schema Layer of a file. This includes Table Definitions, Field Definitions, and the Relationship Graph. Beyond that, Privileges can vary widely, from extensive to highly restricted.

i. Tables
ii. Fields
iii. Relationship Graph

How did this manifest itself? It was occasioned by the appearance of the ***Manage Database*** option that could then be activated by the *Subordinate Level User*. This has existed as far back as FileMaker® Pro 7.

The Triggering Mechanism for this was a Script set to ***Run Script With Full Access Privileges*** and Dialog option set to ***On***. At least four separate Script steps could trigger this:

i. *Export*
ii. *Import*
iii. *Sort*
iv. *Manage Value Lists* (Dialog option not applicable)

```
1
2  Export Records [ With dialog: On ]
3
4
5  Import Records [ With dialog: On ]
6
7
8  Sort Records [ With dialog: On ]
9  Open Manage Value Lists
```

Figure 1. Scripts Steps In Scripts Set To Run With Full Access Privileges

How might a *Subordinate Level User* access such Scripts in a file?

i. Access could be provided in the User Interface of the file by the Developer.
ii. Accessed and triggered from an external file if other proper protections were not in place:
    a. These include principally *File Access Protection, fmurlscript,* and, *fmextscriptaccess*.[3]

This situation ensues principally from the indiscriminate use of *Run Script With Access Privileges* instead of the use of correctly designed Privilege Sets. Wim Decorte discussed this issue in his Engage 2024 presentation.[4]

This is the way the process worked. We will use the *Manage Value List*s Script step as an example here.

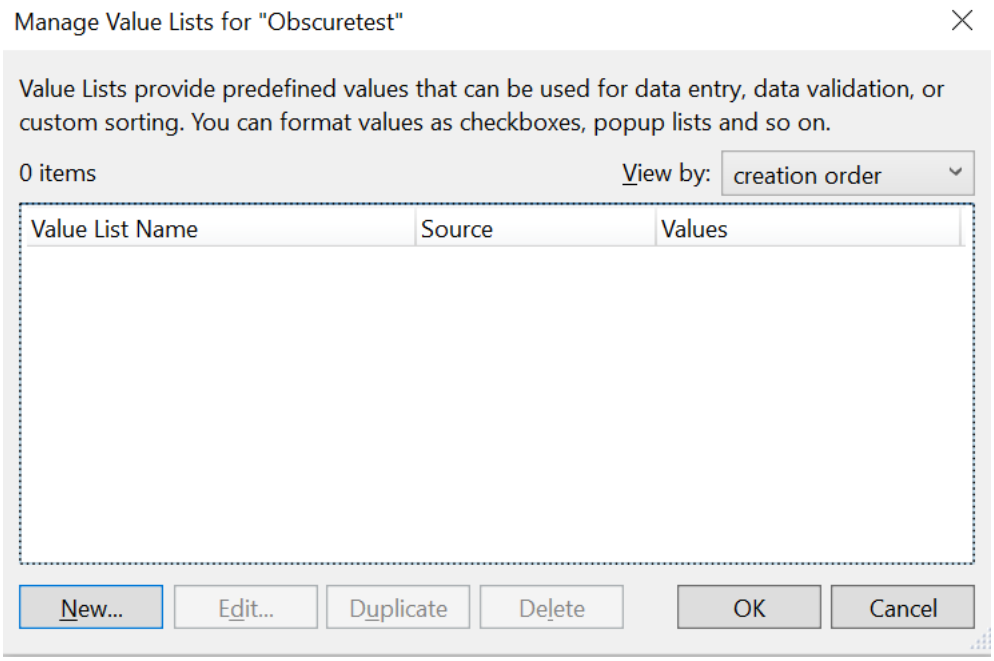

Figure 2. Dialog Opens For Manage Value List

When the Script launches, FileMaker Pro presents the user with a dialog allowing creation of a new Value List.

[3] To prevent unauthorized manipulation by ActiveX or Apple events.

[4] https://community.claris.com/en/s/engage/claris-engage-recordings?vtui__catalogId=a5NVy00000000Cv,a5NVy00000000w5MAA

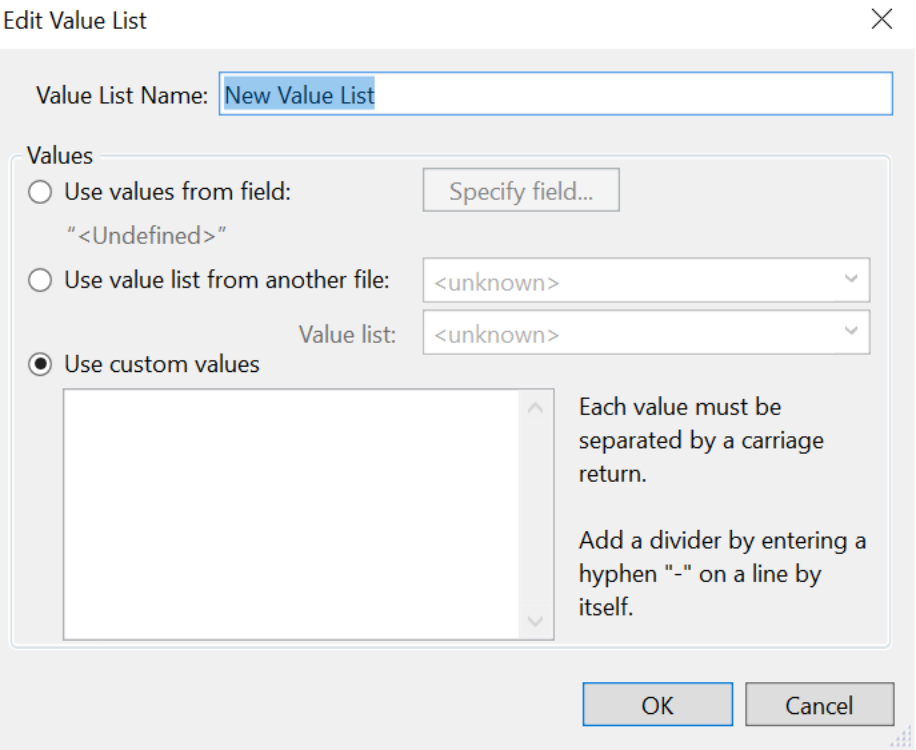

Figure 3. Dialog Opens For Value List Name

After selecting creation of a new Value List, the user sees this Dialog. Focus on the option to "*Use values from field:"* and "*Specify field…*" and then select *Specify.*

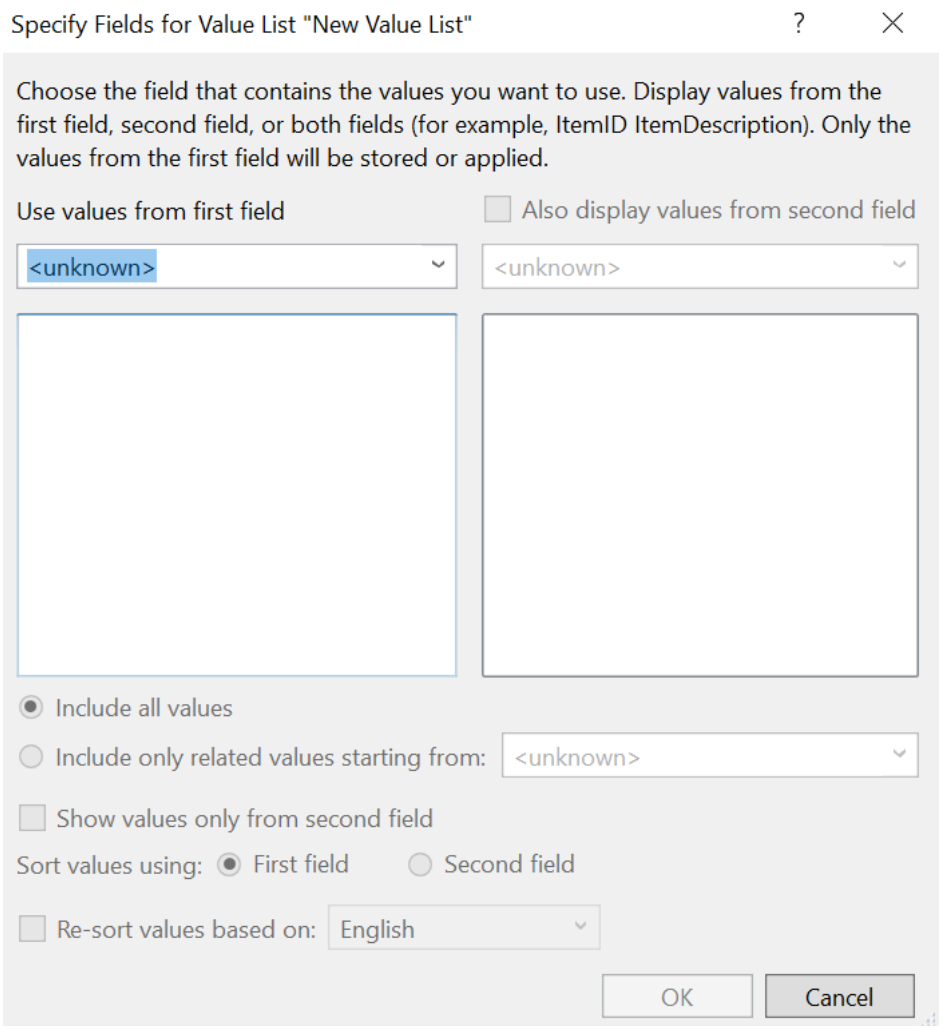

Figure 4. Dialog Opens For Selecting Field

Select the drop-down arrow to the right of the value labeled <*unknown*> and activate it.

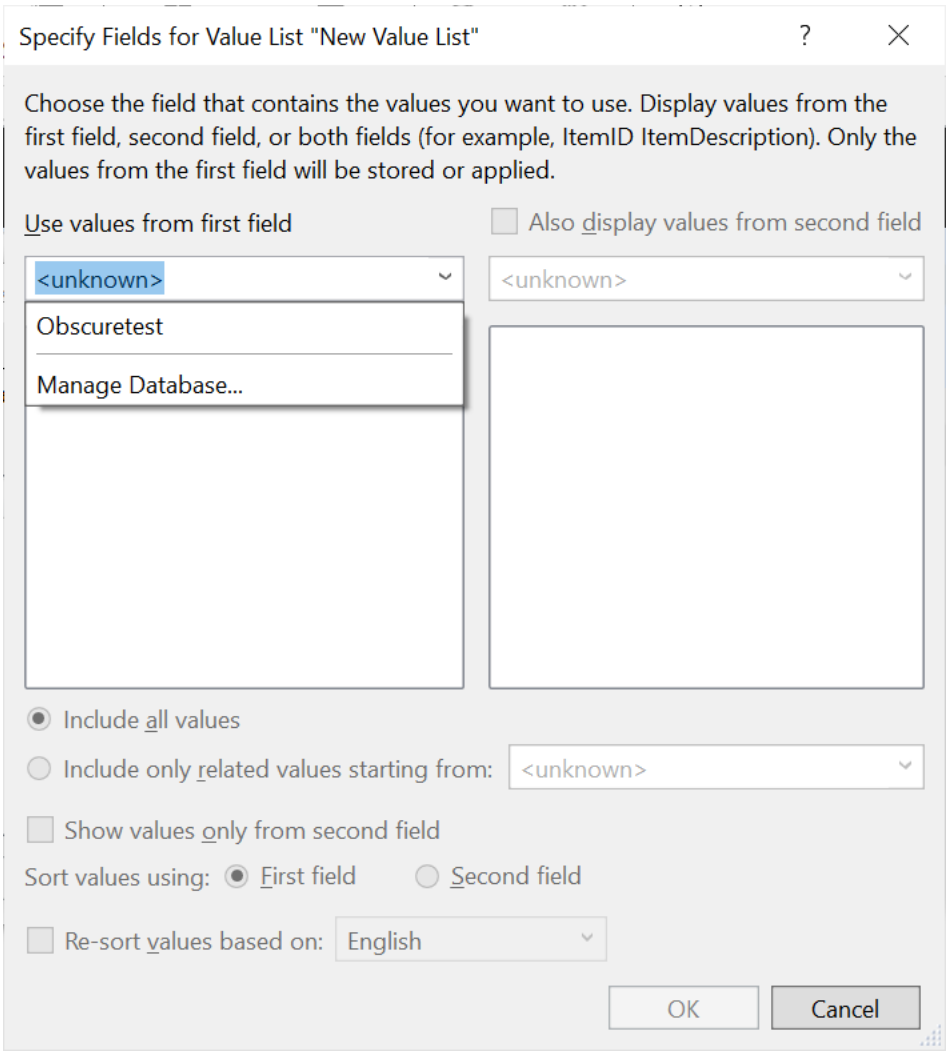

Figure 5. Dialog Opens For Selecting Field And Manage Database Appears

That selection now exposes the option for "***Manage Database…"*** and the *Subordinate Level User* can select it.

The Subordinate Level user is now in the ***Manage Database*** portion of the FileMaker Pro file as shown by the following four illustrations.

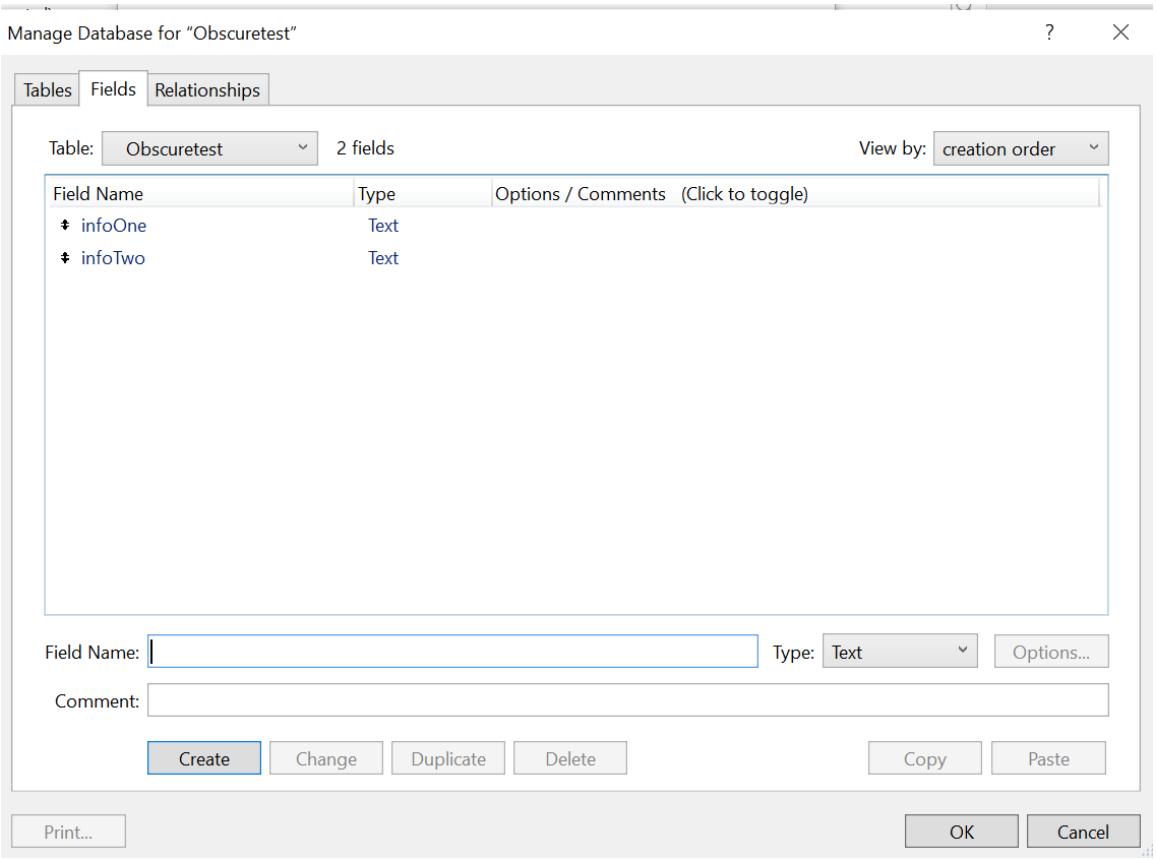

Figure 6. The Manage Database Dialog Opens With Field Options Accessible

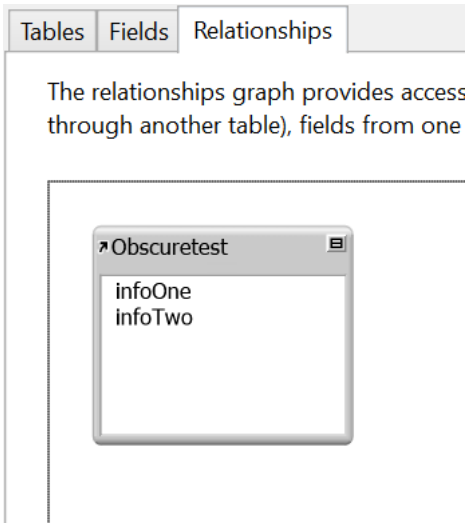

Figure 7. Tables, Field, and Relationships Are Now Accessible

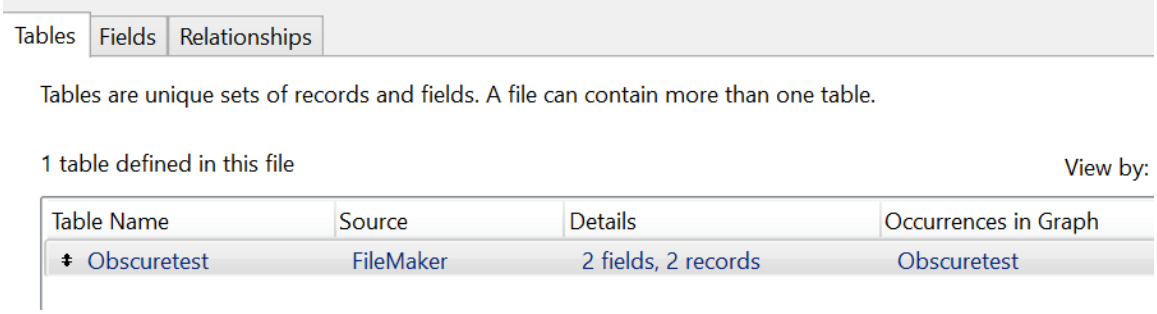

Figure 8. Tables Are Also Accessible

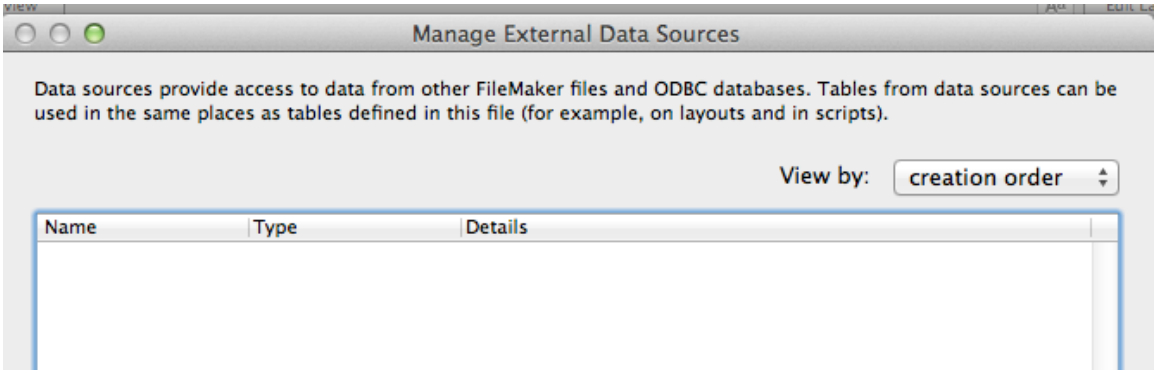

Figure 9. Manage External Data Sources Is Also Now Available.

All this started because the Script that was run with *Full Access Privileges* exposed the *Manage Database* option and the *Subordinate Level User* could trigger it.

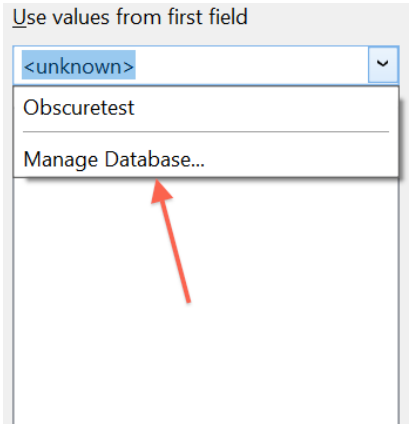

Figure 10. Manage Database Option Previous Versions Enabled

—ADDRESSING THE VULNERABILITY—

So, how was this vulnerability addressed in the new version of FileMaker Pro? The ability to activate the ***Manage Database*** option in these scenarios was ***disabled***. Following through the same process as before in the ***Manage Value Lists*** Script Step now brings the *Subordinate Level User* to a *different ending point.* The *Manage Database* option here no longer works.

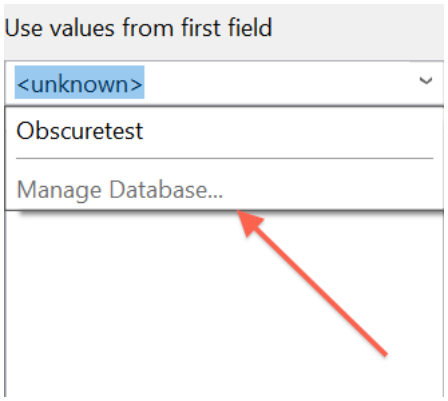

Figure 11. Manage Database Option Now Disabled

This amelioration ***does not mean*** that the option *purposely* to grant a *Subordinate Level User* the ability to access *Manage Database via* script step run with *Full Access Privileges* was removed. Developers can still include this option if they choose to do so. However, we would recommend that they seriously weigh the risks *versus* the benefits of such a move. It is the ***inadvertent access*** that was constrained in this fix.

There are also some additional alternative scenarios for managing this situation:

i. Avoid the indiscriminate use of ***Run Script With Full Access Privileges*** for these four Script Steps.
ii. Do not invoke the *Dialog ON* option.
iii. *Avoid the Manage Value List* option. Use a *Table of Values* instead.

UNEXPECTED ACCESS TO WATCH TAB OF DATA VIEWER

The second vulnerability addressed in the new version is somewhat similar to the first one. This one relates to unexpected access to the ***Watch Tab*** of the ***Data Viewer***.

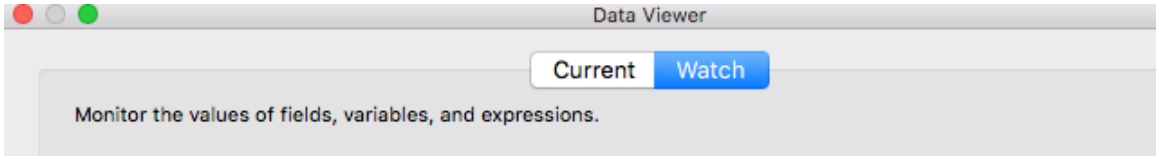

Figure 12. Data Viewer Watch Tab

What is the issue here? The ***Watch Tab*** could be exposed along with its contents to a *Subordinate Level User*. This could expose contents of fields to unauthorized persons.

Additionally, an attacker could change the content of local and global variables, which can lead to privilege escalation if an ***ersatz security system*** is being used where "security" elements are stored in variables. Moreover, with the use of FQL (FileMaker SQL for its metatables) an attacker could extract the whole data dictionary and all data. With the use of a plugin capable of SQL an attacker also could alter and add table and field schema and modify data. This situation has been around since at least Version 12.

What are the Triggering Mechanisms for this scenario? There are several:

i. The same scenarios as the ***Manage Database*** issue described earlier in this White Paper with the four Script Steps.
ii. A Script run with *Full Access Privileges* containing the *Show Custom Dialog Script* Step.
iii. A Script run with *Full Access Privileges* containing the *Pause/Resume Script (Indefinitely)* Script Step.

```
Show Custom Dialog []
```

Figure 13. Show Custom Dialog Script Step

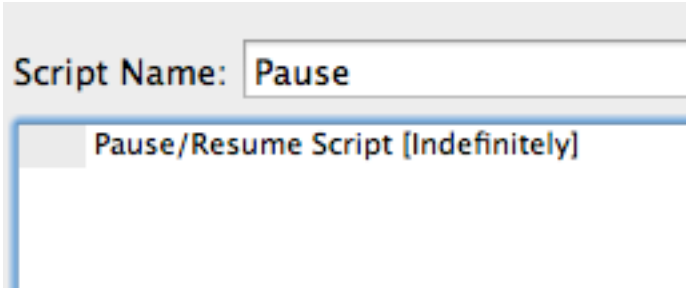

Figure 14. Pause/Resume (Indefinitely) Script

This vulnerability was resolved by *preventing the exposure* of the Watch Tab.

There are also some additional scenarios for managing this situation:

i. Avoid indiscriminate use of *Run Script With Full Access Privileges* for the *original four* script steps or the *Custom Dialog* or the *Pause/Resume Script* one.
ii. Do not invoke the *Dialog ON* option.
iii. Do not allow access to Advanced Tools, preferably through blocking them with the *Assisted Install* options.

ADDITIONAL SECURITY ISSUES ADDRESSED

Claris has recently reported some other Security remediations for the FileMaker Platform in a series of recent patches. We are including these here for reference by Developers. The first two are related to *Client-Server communication*:

i. Tech Info # 000041296[5]
ii. Tech Info # 000041674[6]

Also, two other items related to *Administrator Role* have been previously addressed and reported by Claris:

i. https://support.claris.com/s/article/Administrator-role-passwords-being-exposed-when-logged-into-the-Admin-Console?language=en_US
ii. https://support.claris.com/s/answerview?anum=000041424&language=en_US

Developers should consult these articles, even though they do not contain a great deal of detail.

[5] https://support.claris.com/s/article/FileMaker-Security-Information?language=en_US

[6] https://support.claris.com/s/answerview?anum=000041674&language=en_US

SUMMARY

In this White Paper we have endeavored to report on the remediation in the new version of FileMaker Pro of two significant and unexpected *Escalation of Privileges* vulnerabilities. We have explained what they were and how they might be triggered. And we have explained how the new version remediates these two items.

We have also stressed the importance of employing the full suite of Security Tools available in the FileMaker Platform **in order to imbue the FileMaker Pro files with the most widespread and effective Security the Platform can offer.**

We invite the close attention of members of the FileMaker Developer Community to these items.

##################

—About The Authors—

Wim Decorte is the Director of the Claris Practice at Soliant Consulting Inc., a Claris Platinum Member company. He is a leading expert on FileMaker Server, FileMaker Platform integration, and IT infrastructure issues. He is the author of numerous White Papers, Technical Briefs, and BLOG posts.

Steven H. Blackwell is a Platinum Member Emeritus. He is the author of *FileMaker Security: The Book* as well as numerous White Papers and Technical Briefs about FileMaker Platform Security. He is also the creator of the FileMaker Security BLOG (http://fmforums.com/blogs/blog/13-filemaker-securityblog)