

Securing Your FileMaker Server

Last Modified on 10/30/2026 5:20 pm EDT

This guide explains security precautions to implement due to recent FileMaker Server attacks. It is intended for system administrators and IT specialists.

For AI-powered threats targeting FileMaker and other technology platforms, there are several security precautions aACE Software recommends implementing. In October 2026, Claris hosted a webinar addressing recent AI attacks on FileMaker servers with recommendations for security precautions.

aACE Software has no reason to believe that aACE 6 is significantly vulnerable to these recent attacks. However, we have both optional and recommended precautions for the immediate and near term.

Table of Contents

- [What We Know, aACE 6, and Our Next Steps](#)
- [Immediate Action Items](#)
- [Short Term Action Items](#)

What We Know, aACE 6, and Our Next Steps

The Claris October 2026 security webinar explains attack methods. Here are some essential details from the webinar as they pertain to FileMaker Server:

- The attacks seek to access files through the FileMaker Data API. Therefore, disabling the Data API blocks this particular attack vector.
- The attacks target specifically-named files that permit access through a guest account or other forms of automatic authentication.
- The attacks seek to extract data through specifically-named layouts.
- If an attacker is successful, they might gain access to data contained in fields accessible through those layouts, subject to the file's security configuration.

aACE Software is confident that aACE 6 solutions are not significantly vulnerable to these reported attack methods because we do not use a guest account or automatic authentication for aACE data files. However, aACE does have a number of files that use a

guest account for automatic authentication. These files either present aACE data in a particular way (e.g. Reports) or transmit aACE data from the data file to a third party (e.g. our integrations). If these files that use a guest account are compromised, they are not very useful to an attacker.

However, some of these files that use a guest account temporarily retain small amounts of data cached as part of recent transactions. If any of these files were compromised and cached data were exposed, an attacker's access would be constrained by the file's security configuration, including the fields accessible through its layouts. As a matter of practice, we include relatively few fields on the layouts in these files, and any cached data is retained only for a short period of time. An attacker would also need to identify these relevant files and layouts.

aACE Software intends to complete the following items in the short term:

- Audit each of our integrations and conduct further penetration testing
- Update all of our Reports and integration files to use credential-based authentication.
- Coordinate these updates during a scheduled security review with your team, prioritizing customers who rely on the Data API and therefore cannot disable it in the immediate term.

[Top](#)

Immediate Action Items

As a customer, there are some actions you are able to complete while we perform our piece. To take immediate action, aACE Software recommends disabling the Data API and determining if your server was targeted during the attacks.

Disabling the Data API

The most effective way to secure your FileMaker Server against the attack methods Claris mentioned is to disable the FileMaker Data API. aACE does not generally rely on the Data API except for mobile apps. If you are not using any of our mobile apps and are not aware of any custom services that require it, we suggest disabling the Data API. It is important to note that there might be some risk to disrupting existing functionality.

If you are using any of our mobile apps or have services that rely on the Data API, you cannot disable the Data API yourself. In the meantime, there are actions you can perform until we can assist during your scheduled security review. We will then prioritize security

reviews for customers with mobile apps or custom services that require the Data API.

Customers Without Mobile Apps

If you do not use mobile apps or are aware of any custom services that require the Data API, disable the Data API for your system:

1. Log in to the FileMaker Server Admin Console.
2. Go to **Connectors > FileMaker Data API**.
3. Disable **FileMaker Data API**.

Customers With Mobile Apps

If you use mobile apps or have custom services that require the Data API, ensure Data API Logging is enabled:

1. Login to the FileMaker Server Admin Console.
2. Go to **Logs > Log Settings**.
3. Enable **Allow FileMaker Data API Script Log**.

The FileMaker Data API Database Names endpoint now requires authentication credentials when the following items are both enabled:

- The Filter Database in Client Applications option
You can enable this by going to Configuration > Clients > Filter databases in client applications
- The DenyGuestAndAutoLogin preference
You can enable this by entering the following command to a Command Line Interface:

Plain text

```
fmsadmin set serverprefs DenyGuestAndAutoLogin=true
```

Determining If Your Server Was Targeted

More technical details regarding the current threat are provided below. However, you can determine whether your server might have been targeted by an attack:

- Examine the FileMaker Server "Event.log" file for an increase in unsuccessful login attempts, noting repeated authentication errors (Event ID 661).

Attackers might make 15–20 attempts before temporarily stopping and resuming from a different IP address, so note recurring bursts of activity separated by periods of inactivity. These attacks are likely to be conspicuous rather than subtle. Keep in mind that failed login attempts can occur during normal operations and do not necessarily indicate a compromise.

- Investigate attempts from unfamiliar IP addresses (e.g. 76.71.171.67, an identified attacker IP). Record source IPs, timestamps, event types, and attempt frequency to identify patterns.
- If you identify any suspicious IP addresses, search for other activity from the same addresses in the other logs, such as FileMaker Server Access, Data API, OData, and Web Publishing Engine (WPE), as available.

If you require assistance, contact our team at support@aacessoft.com.

[Top](#)

Short Term Action Items

The recent attacks do not appear to exploit vulnerabilities in PHP or FileMaker Server itself. However, the following actions should be taken in the short term (i.e. November) to address other ongoing attacks (e.g. PHP2Shell) and legacy vulnerabilities that have been resolved in more recent versions of FileMaker Server.

Disabling or Removing PHP

aACE does not require PHP for your FileMaker Server. If you are not aware of any custom solutions or services that require PHP, your IT professional should disable or remove it. Otherwise, make immediate arrangements to apply necessary security patches.

Upgrading FileMaker Server

Older versions of FileMaker Server should be upgraded to FileMaker Server 26. If you are uncertain about the appropriate next steps, contact support@aacessoft.com.

Performing a Security Review

During the first two weeks of November 2026, aACE team members are available to meet with your team (i.e. system administrators and IT professionals) to review your aACE server

and its configuration, any custom solutions or services you might have, and other pertinent topics. Our aACE team members have reserved time on our calendar every Monday through Friday at 9 AM ET, 1 PM ET, and 3 PM ET. We will prioritize customers who are unable to disable the Data API.
