

Security Information

There will be security information that needs to be shared about FileWave or components that we use. We may also link to critical notices about macOS, Windows, iOS, and other OSs if they appear to be severe, and would impact you as an IT manager.

- [FileWave Security](#)
- [Supply-Chain Attack Threat Management](#)
- [Apache CVE-2006-20001 / CVE-2022-36760 / CVE-2022-37436](#)
- [Security Notice: Apache log4j Vulnerability CVE-2021-44228](#)

FileWave Security

FileWave SSL Certificates

Using self-signed certificates should be avoided as much as possible in production environments; while it may make sense in some closed environments, using Globally trusted CAs is our recommended approach.

The FileWave Server and other FileWave Components (e.g. Clients, Web Console, IVS, etc.) use the MDM server SSL certificate to validate communication. This certificate needs to be uploaded into the SSL Certificate Management pane, in the General tab inside FileWave Admin Preferences. This validation check will ensure secure and trusted communication between your FileWave server and the various FileWave components in your environment. Even though a self-signed certificate is supported, having a root trusted certificate from a CA is the best and most recommended option.

- [For more information on creating a root trusted certificate](#)
- [How your FileWave environment will be affected by have a self-signed certificate](#)
- [Let's Encrypt Setup for FileWave Server \(Debian\)](#)

Security and FileWave

FileWave uses SSL, certificates, and secure tokens for much of its primary device and content management. Fileset technology is a patented, proprietary wrapper for content. Instead of sending a standard .pkg or .msi installer packages to the client, we wrap the content inside a Fileset. Because this is a proprietary container, the integrity of the delivered content is assured.

FileWave client security

Communications between the FileWave Client and either the Server or any Boosters is done through SSL.

The FileWave Client is tracked by device name in Inventory. Admin changes to Client configurations are either done through a specific Fileset, called a Superprefs Fileset, or through the Client Monitor. The contents of a Superprefs Fileset are secure from external packet sniffing, package viewer tools, and brute force access. The Client Monitor settings are protected by a unique password assigned by the FileWave Admin at the time of installation of the FileWave client. This password is not readily available to the device's local administrator.

FileWave Server security

The FileWave client communicates to the FileWave Server using SSL. The FileWave server supports multiple sub-administrators. The biggest concern is proper password and account management; but each sub-admin can be limited as to their level of access to clients, Filesets, and services.

- [Securing FileWave Server on the Internet for Remote Device Management](#)

Client tracking

A device can be tracked from FileWave Admin. Activating tracking involves setting the client state of the device to Normal and the current user of the device will receive a notification asking them to approve tracking (iOS and OS X only). Android devices will request that all client permissions be granted at installation, and Windows devices do not provide any user notification. Only devices on Wi-Fi will be tracked.

These tracking options can be disabled for any FileWave administrator account by modifying their permissions in the FileWave Admin. You can also have a global change on your FileWave license by requesting to disable Personal Data Collection. Keep in mind, disabling Personal Data Collection will not only prevent FileWave from gathering location data but also other personal data on the device.

Disaster recovery

Backup of both the server environment and end user data are critical areas of planning. Backup of your servers can be as simple as taking snapshots of the VMs at regular intervals. The FileWave server is running a database using SQL, and as such, you cannot use normal backup solutions to insure its safety. Use the information on the FileWave Support site to make sure you properly back up the server.

- [Automated Backup](#)

Supply-Chain Attack Threat Management

QUESTION

How well is FileWave's product protected against Supply-Chain Attacks? What efforts does FileWave make to protect against this threat?

ANSWER

Supply-Chain Attacks represent an attack vector that is especially sensitive to software vendors that produce systems used in ITSM. As one of the leading UEM vendors in cross-platform device management, FileWave is constantly working on improving our processes and tooling to make sure that our product is protected against known, material vulnerabilities.

Supply Chain attacks can be difficult to detect and respond to due to the fact that a vulnerability can be introduced at multiple points during the time of product creation, release and delivery process and can originate both within the company or come through a previously trusted, upstream source - e.g. partner product , a library or an OSS component.

To reduce the possibility of such breach and be able to react quickly, we are pursuing a number of complementary activities, which allow us to control the source of the components and libraries used in releases, automate the process of the product assembly thus limiting possibility for human error and oversight, and solicit feedback from security experts and communities.

No security process is perfect however, so we stay diligent and always look for improvements in our tools and processes, especially in response to ever evolving cybersecurity threats and attack methods.

ADDITIONAL INFORMATION

[Open Source Software Included in FileWave](#)

Apache CVE-2006-20001 / CVE-2022-36760 / CVE-2022-37436

What

On January 17, 2023, Apache released version 2.4.55 to address three vulnerabilities (CVE-2006-20001/CVE-2022-36760/CVE-2022-37436).

When/Why

Our development team has reviewed these vulnerabilities and found that FileWave is not vulnerable to any of them.

How

Two of the modules are not used and the third module exploit is not relevant for our implementation. We plan to incorporate Apache version 2.4.55 or later in the next possible release.

Related Links

- https://httpd.apache.org/security/vulnerabilities_24.html

Security Notice: Apache log4j Vulnerability CVE-2021-44228

Info

From December 9, 2021 reports of a Zero Day exploit for Apache Log4j 2.x <= 2.15.0-rc1 were being reported in the wild under CVE-2021-44228.

Question

Are FileWave systems impacted by this exploit?

Answer

FileWave at one point in time (more than 4 years ago) did use log4qt, a C++ implementation of log4j, but its use was discontinued from version 12.4 of FileWave. The Java version of log4j was never used by FileWave. Therefore FileWave systems (Boosters, Server, IVS, and Clients) are NOT impacted by this vulnerability.