

Securing FileWave Server on the Internet for Remote Device Management

What

This article provides guidance on securely exposing and managing your FileWave server on the internet for remote device management.

When/Why

You might need to expose your FileWave server on the internet to manage devices anywhere they might be, including performing actions like remote wipes. However, this must be done carefully to ensure the security of your server.

How

1. Limit Exposed Services: Consider what services are exposed. For instance, on CentOS VM appliances, WebMin runs on port 10000. It's recommended not to expose this to the internet. Similarly, block SSH to prevent unauthorized access.
2. Allow Only Necessary Ports: Only allow the FileWave ports that are necessary. Refer to the TCP and UDP ports KB article for the list of ports used by FileWave.
3. Apply OS Patches Consistently: Ensure that operating system patches are applied consistently. For CentOS, this means running `yum update` followed by `yum upgrade`. Reboot the server if a kernel update is applied.
4. Use Complex Passwords: Make sure that the root password on Linux or any passwords for the operating system at all for both macOS and Linux for the FileWave server are complex. This makes it harder for unauthorized users to gain access.
5. Implement Two-Factor Authentication (2FA): Enable two-factor authentication for accessing the FileWave server. This provides an additional layer of security by requiring users to provide a second form of authentication, such as a unique verification code sent to their mobile device. FWAdmin is always present so set that user to an extremely long and complex password.
6. Enable Firewall and Intrusion Detection System (IDS): Configure a firewall to filter incoming and outgoing traffic, allowing only necessary connections. Additionally, set up an intrusion detection system to monitor and alert you about any suspicious activities on your server.
7. Regularly Monitor Server Logs: Continuously monitor the server logs for any signs of unauthorized access attempts or unusual activities. Implement a log management solution to centralize and analyze log data for better security monitoring. This is difficult to do manually, so look at security monitoring tools.
8. Apply FileWave Upgrades: Keep your FileWave server up to date by applying FileWave upgrades when they are released. These upgrades often contain security updates, especially for third-party open-source software like Apache and OpenSSL, which can include critical updates.

Related Links

- [TCP and UDP ports used by FileWave](#)
- [Allow External Devices to Connect to the FileWave Server and Boosters](#)
- [How to Disable Apache Version Number Disclosure on FileWave Server](#)

Note: As we move to the next Linux distribution, the guidance will remain the same. This article will be updated with additional recommendations as they are identified.

Remember, security is a continuous process. Always monitor your server for suspicious activity, keep your system up to date, and follow best practices to ensure the integrity and confidentiality of your FileWave server.

🔄Revision #5

★Created 5 July 2023 20:03:45 by Josh Levitsky

🔧Updated 16 July 2023 23:57:04 by Josh Levitsky