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

Revision #1
★Created 21 June 2023 19:50:52 by Josh Levitsky
✎Updated 12 July 2023 01:39:12 by Josh Levitsky