REPRODUCIBLE BUILDS

Protecting software integrity with verifiable releases

Overview

With a growing threat landscape, organizations are increasingly seeking solutions to defend against software supply chain attacks and eliminate points of vulnerabilities in the software development process. One approach to protecting software integrity is to verify releases during the build process.

"Releases" is a DigiCert Software Trust Manager feature that reduces the risk of malware or spyware injection in production software by leveraging reproducible builds or deterministic compilation as part of a software supply chain security framework. With Releases, organizations can verify build artifacts by performing commit signing and comparing hashes from binaries compiled from the same source in different build environments.

The Releases feature protects the integrity of production software by capturing any discrepancies in the output binaries. In addition, Releases provides strong controls in keypair and signing assignments, preventing unauthorized signing activities for software builds.

Key Benefits

- Reduce the risk of malware injection during the build process by verifying build artifacts against a baseline release
- Prevent unplanned signing & release activities, with centrally enforced keypair and signing controls on releases
- Use insights from software builds to refine processes to eliminate malicious artifacts

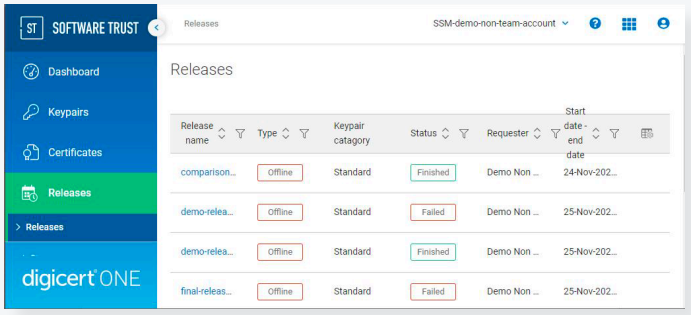
Key Features

Adopt software supply chain security framework best practices
Enables commit signing. Generates and compares test releases using hashes to create the baseline or production release.

Implement granular controls on keypairs and signing
Supports keypair usage restrictions such as preapproved dates and times (release window), authorized keypairs, and authorized signers. Ensures releases are only associated with signatures from authorized signers.

Halt irregular builds
Discontinues build process automatically for non-matching artifacts until issues are resolved.

Report on and analyze build artifacts
Generates analysis of all release comparisons to provide insights on build factors for matching and non-matching artifacts.



The Releases feature of DigiCert Software Trust Manager supports reproducible builds and enforces keypair and signing controls, reducing the risk of malware injection and protecting software integrity.