Keeper Security Protects Against Supply Chain Attacks with New Open Source Project

Keeper Secrets Manager can now securely sign git commits using SSH keys protected in the Keeper Vault

LONDON, UNITED KINGDOM, October 18, 2023 /EINPresswire.com/ -- Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, today announces a new open source project for software developers and DevOps to easily and securely sign git commits with their Keeper vault. Through Keeper Secrets Manager (KSM), users can now use Secure Shell (SSH) keys stored in their Keeper Vault to digitally sign commits to confirm the authenticity of their code.

Git is a version control system that tracks changes in your software projects, and a git commit is a snapshot of these changes at a specific point in time, accompanied by a brief message describing the modifications. Keeper and developers at The Migus Group teamed up to create the open-source solution to sign git commits using the SSH keys stored in a user's Keeper Vault. The integration provides developers with a secure and encrypted repository for their SSH keys and removes the practice of storing them on disk, both increasing security and streamlining DevOps workflows.

The rise in software supply chain attacks highlights the need for organisations to prioritise security around the software supply chain. Signing git commits is a recommended best practice for developers to confirm the authenticity and integrity of code releases. As developers sign commits with SSH keys, they are provided with cryptographic proof of authorship, which helps secure the supply chain by assuring users the software originates from a legitimate source and remains unaltered since its signing. Digital signatures can also feed into a Software Bill of Materials (SBOM) to indicate whether a line-item in the SBOM is trusted, depending on the code signature status.

“The ability to store SSH keys and other credentials in Keeper Vault offers a layer of protection and ease-of-use that hasn’t been the standard,” said Craig Lurey, CTO and Co-founder of Keeper Security. “Our integration enables developers to validate the software code with a cryptographic digital signature and transparent logging, making what historically has been a complex process into a simple one. In the future, all code will be signed, and the software supply chain will have one source of truth that will reduce supply chain attacks.”

"Our customers are asking for help insulating themselves from supply chain attacks, so we were already working to do that, often using Keeper," said Adam Migus, Founder and CEO of The Migus Group. "so, we thought working with them to make the git commit-signing process both safer and easier would be a win-win-win. Our customers can now seamlessly sign commits with keys that never leave their vaults. However, the broader community also gains an example of secure commit signing with benefits of central key management."

The SSH keys for signing commits are secured in KSM, a fully managed cloud-based, zero-knowledge platform for securing infrastructure secrets such as API keys, database passwords, SSH keys, certificates and any type of confidential data. KSM eliminates secrets sprawl by removing hard-coded credentials from source code, config files and CI/CD systems. The fully managed, cloud-based and IT friendly solution was named an overall leader on the 2023 KuppingerCole Leadership Compass for Secrets Management. KSM is supported on Windows, MacOS and Linux. It utilises a zero-knowledge security architecture and is highly secure withISO 27001 and SOC 2 compliance, as well as FedRAMP and StateRAMP Authorization, among numerous other certifications.

Keeper’s integration helps support a broader government and industry effort to bring increased security and visibility to the open source community. The ease of providing a cryptographic digital signature allows developers to validate that the software in use is exactly what it is claiming to be and enhances security for both developers and end-users alike.

Learn more about how KSM can help users sign git commits.

About Keeper Security
Keeper Security is transforming cybersecurity for people and organisations around the world. Keeper’s affordable and easy-to-use solutions are built on a foundation of zero-trust and zero-knowledge security to protect every user on every device. Our next-generation privileged access management solution deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by millions of individuals and thousands of organisations, Keeper is the leader for best-in-class password and passkey management, secrets management, privileged access, secure remote access and encrypted messaging. Learn more at KeeperSecurity.com.

Charley Nash
Eskenzi PR

charley@eskenzipr.com