# Keeper Security schützt mit neuem Open-Source-Projekt vor Angriffen auf die Software-Lieferkette

*Keeper Secrets Manager kann jetzt Git-Commits mit SSH-Schlüsseln sicher signieren und im abgesicherten Keeper Vault schützen*

**München, 18. Oktober 2023 –** Keeper Security, führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, kündigt heute ein neues Open-Source-Projekt an. Damit können Softwareentwickler und DevOps Git-Commits einfach und sicher mit ihrem Keeper Vault signieren. Mit dem Keeper Secrets Manager (KSM) können Anwender nun Secure Shell (SSH)-Schlüssel, die in ihrem Keeper Vault gespeichert sind, verwenden, um Commits digital zu signieren und so die Authentizität ihres Codes zu bestätigen.

Ein Git-Commit ist ein Versionskontrollsystem, das Änderungen in Softwareprojekten verfolgt. Ein Git-Commit ist ein Snapshot der Änderungen zu einem bestimmten Zeitpunkt festhält, begleitet von einem kurzen Bericht, der die Anpassungen beschreibt. Keeper und die Entwickler von The Migus Group kooperieren, um eine Open-Source-Lösung zum Signieren von Git-Commits mit SSH-Schlüsseln zu entwickeln, die im Keeper Vault eines Benutzers gespeichert sind. Die Integration stellt Entwicklern ein sicheres und verschlüsseltes Repository für ihre SSH-Schlüssel zur Verfügung und eliminiert die Praxis, diese auf der Festplatte zu speichern, was sowohl die Sicherheit erhöht als auch die DevOps-Workflows verbessert.

Die Zunahme von Angriffen auf die Software-Lieferkette unterstreicht die Notwendigkeit für Unternehmen, die Sicherheit zu priorisieren. Das Signieren von Git-Commits ist eine empfohlene Best Practice für Entwickler, um die Authentizität und Integrität von Code-Releases zu bestätigen. Wenn Entwickler Commits mit SSH-Schlüsseln signieren, erhalten sie einen kryptografischen Nachweis der Urheberschaft, der zur Sicherheit der Lieferkette beiträgt, indem er den Benutzern versichert, dass die Software aus einer legitimen Quelle stammt und seit der Signierung unverändert geblieben ist. Digitale Signaturen können auch in eine Software Bill of Materials (SBOM) einfließen, um anzuzeigen, ob eine Position in der SBOM je nach dem Status der Codesignatur vertrauenswürdig ist.

„Die Möglichkeit, SSH-Schlüssel und andere Berechtigungsnachweise in Keeper Vault zu speichern, bietet eine Ebene des Schutzes und der Benutzerfreundlichkeit, die bisher nicht üblich war", so Craig Lurey, CTO und Mitbegründer von Keeper Security. „Unsere Integration ermöglicht es Entwicklern, den Softwarecode mit einer kryptografischen digitalen Signatur und einer transparenten Protokollierung zu validieren, wodurch ein bisher komplexer Prozess zu einem einfachen wird. In Zukunft wird der gesamte Code signiert sein, und die Software-Lieferkette wird eine einzige, valide Quelle haben, die Angriffe auf die Lieferkette reduziert."

„Unsere Kunden bitten uns um Hilfe, um sich vor Angriffen auf ihre Lieferkette zu schützen, und wir haben bereits daran gearbeitet, oft unter Verwendung von Keeper", sagt Adam Migus, Gründer und CEO von The Migus Group. „Daher sind wir überzeugt, dass eine Zusammenarbeit mit Keeper, um den Git-Commit-Signierungsprozess sowohl sicherer als auch einfacher zu machen, eine Win-Win-Win-Situation ist. Unsere Kunden können jetzt nahtlos Commits mit Schlüsseln signieren, die ihren Tresor nie verlassen. Aber auch die breitere Community erhält ein Beispiel für sicheres Commit-Signing mit den Vorteilen einer zentralen Schlüsselverwaltung."

Die SSH-Schlüssel für das Signieren von Commits werden in Keeper Secrets Manager KSM gesichert. KSM ist eine vollständig verwaltete, Cloud-basierte Zero-Knowledge-Plattform zur

Sicherung von Infrastrukturgeheimnissen wie API-Schlüsseln, Datenbankpasswörtern, SSH-Schlüsseln, Zertifikaten und jeder Art vertraulicher Daten. KSM beseitigt den Wildwuchs an Geheimnissen, indem es hart kodierte Anmeldeinformationen aus Quellcodes, Konfigurationsdateien und CI/CD-Systemen entfernt. Keeper wurde mit der Lösung im 2023 KuppingerCole Leadership Compass for Secrets Management als einer der führenden Anbieter ausgezeichnet. KSM unterstützt Windows, MacOS und Linux. Die Lösung nutzt eine Zero-Knowledge-Sicherheitsarchitektur und ist hochsicher mit ISO 27001- und SOC 2-Konformität sowie FedRAMP- und StateRAMP-Autorisierung sowie zahlreichen anderen Zertifizierungen.

Die Integration von Keeper unterstützt die Bemühungen von Regierung und Industrie, der Open-Source-Community mehr Sicherheit und Transparenz zu bieten. Die einfache Bereitstellung einer kryptografischen digitalen Signatur ermöglicht es Entwicklern, zu überprüfen, ob die verwendete Software genau das ist, was sie zu sein vorgibt, und erhöht die Sicherheit für Entwickler und Endbenutzer gleichermaßen.

Erfahren Sie mehr darüber, wie KSM Benutzern beim Signieren von Git-Commits helfen kann.

**Über Keeper Security Inc.**
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie mehr unter KeeperSecurity.com.

**Pressekontakt für Keeper in DACH:**
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de