KEEPER | Pressemitteilung

Keeper Security unterstützt Entwickler mit sicherer Geheimnisverwaltung in Visual Studio Code

Die Zero-Trust- und Zero-Knowledge-Erweiterung von Keeper ermöglicht Entwicklern sicheres Programmieren, ohne ihren Arbeitsablauf unterbrechen zu müssen

MÜNCHEN, 17. November 2025 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern und Passkeys, Infrastrukturgeheimnissen, Remote-Verbindungen und Endpunkten, gibt die Einführung seiner Visual Studio Code (VS Code)-Erweiterung bekannt, mit der die unternehmensgerechte Geheimnisverwaltung von Keeper direkt in die Programmierumgebungen von Entwicklern integriert wird. Die VS Code-Erweiterung weitet die KeeperPAM®-Plattform auf das Entwickler-Ökosystem aus und ermöglicht eine sichere Zero-Trust-Geheimnisverwaltung während des gesamten Softwareentwicklungszyklus.

Eine sichere Geheimnisverwaltung ist für Entwickler von entscheidender Bedeutung. Sie schützt die Anmeldedaten, API-Schlüssel, Tokens und Zertifikate, auf die Anwendungen angewiesen sind, um sicher zu funktionieren. Wenn diese Geheimnisse unsachgemäß behandelt werden – z. B. wenn sie im Klartext gespeichert, fest im Quellcode codiert oder informell weitergegeben werden – entstehen schwerwiegende Schwachstellen, die Angreifer ausnutzen können, um Systeme oder Daten zu kompromittieren.

Mit der neuen Keeper VS Code-Erweiterung können Entwickler Befehle unter Verwendung der in ihrem Keeper Vault gespeicherten Geheimnisse speichern, abrufen, generieren und ausführen, ohne ihre Programmierumgebung verlassen oder sensible Informationen in Konfigurationsdateien offenlegen zu müssen. Diese direkte Integration unterstützt sowohl Keeper Commander CLI als auch Keeper Secrets Manager und bietet Unternehmen die Flexibilität, sich an ihre bevorzugte Infrastruktur und Sicherheitsanforderungen anzupassen.

„Entwickler spielen eine entscheidende Rolle bei der Sicherung der Software-Lieferkette“, sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Durch die direkte Integration von Keeper in Visual Studio Code können Teams von Anfang an sicher entwickeln. Mit der Einbettung von Zero-Trust-Prinzipien in ihre Arbeitsabläufe können Entwickler Geheimnisse schützen und die Compliance aufrechterhalten, ohne die Innovation zu verlangsamen.“

Die neue Erweiterung spiegelt das kontinuierliche Engagement von Keeper wider, einheitliche Funktionen für privilegierten Zugriff und Geheimnisverwaltung bereitzustellen, die den sich wandelnden Anforderungen moderner Unternehmen und Entwicklungsteams entsprechen.

Zu den wichtigsten Funktionen der Keeper VS Code-Erweiterung gehören:

- **Geheimnisverwaltung:** Speichern, Abrufen und Generieren von Geheimnissen direkt aus Keeper Vault
- **Flexible Nutzung:** Betrieb im Keeper Commander CLI- oder Keeper Secrets Manager-Modus

- **Geheimniserkennung:** Automatische Identifizierung von fest codierten Anmeldedaten wie API-Schlüsseln und Tokens zur sofortigen Behebung
- **Sichere Befehlsausführung:** Ausführen von Anwendungen mit Geheimnissen, die sicher aus Keeper Vault eingefügt wurden
- **Protokollierungs- und Debugging-Tools:** Anzeigen von Protokollen und Aktivieren des Debugging-Modus für vollständige Transparenz des Betriebs

Durch die direkte Integration der Geheimnisverwaltung in VS Code hilft Keeper Unternehmen dabei, die Verbreitung von Geheimnissen zu reduzieren, versehentliche Offenlegungen zu verhindern und die Compliance mit Zero-Trust- und Least-Privilege-Sicherheitsframeworks aufrechtzuerhalten.

Keeper Secrets Manager ist Teil der Plattform für privilegierten Zugriff von Keeper, KeeperPAM®. KeeperPAM basiert auf einer Zero-Trust- und Zero-Knowledge-Architektur und kombiniert die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit der Verwaltung von Endpunktberechtigungen, Zero-Trust-Netzwerkzugriff und Remote-Browser-Isolation in einer einzigen cloudbasierten Plattform. Keeper Secrets Manager macht die manuelle Verteilung von Geheimnissen überflüssig, erzwingt den Zugriff mit geringsten Berechtigungen und ermöglicht die automatisierte Rotation von Anmeldedaten, wodurch die Sicherheit erhöht und gleichzeitig die Entwicklungsabläufe beschleunigt werden. Mit zentraler Transparenz, detaillierten Prüfpfaden und API-Integrationen, die sich nahtlos in bestehende Tool-Chains einfügen, ermöglicht KeeperPAM Entwicklern ein schnelleres Codieren, sicheres Deployen und die Einhaltung von Compliance-Vorgaben bei minimalem Aufwand.

Die neue Erweiterung von Keeper ist ab sofort sowohl im Visual Studio Marketplace als auch in der Open VSX Registry verfügbar und gewährleistet die Kompatibilität mit VS Code und dessen Derivaten wie Cursor.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64

Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de