Parity Bug friert 130 Millionen Euro ein

Aktuell bereitet eine kritische Sicherheitslücke den Nutzern der digitalen Währung *Ethereum* große Sorgen. *„Parity Technologies“*, das Unternehmen hinter der Krypto-Währung *„Ethereum“*, teilte vor wenigen Tagen mit, dass ein Programmierfehler dazu führte, dass alle Ether-Einheiten in Multi-Signatur-Wallets, die nach dem 20. Juli 2017 erzeugt wurden, nicht mehr transferiert werden können. Laut Experten handelt es sich dabei um Ether-Einheiten mit einem geschätzten Wert von 130 Millionen Euro. Ob ein Zugriff auf diese Einheiten wiederhergestellt werden kann, ist bislang ungeklärt. Wie das Unternehmen mitteilte, wird zurzeit an einer Lösung gearbeitet.

Zusammenfasung

Vor wenigen Monaten sorgte ein Bug in der beliebten Kryptogeldwallet Parity für Aufsehen. Aufgrund eines Fehlers in der Multi-Signatur, konnten Unbekannte in die digitalen Geldbörsen von Nutzern eindringen und schätzungsweise 150.000 Ether-Einheiten im Wert von rund 30 Millionen Euro stehlen. Kurz nach der Veröffentlichung der Sicherheitslücke wurde diese von Parity behoben. Zu dieser Zeit war jedoch nicht bekannt, dass sich in dem Patch ein neuer Bug befand, der als Auslöser für das aktuelle Problem gilt.

Durch einen Fehler in der Programmierung des Patchs, gelang es einem Nutzer, sich Zugriff auf die Code-Bibliothek zu verschaffen.

Anschließend wurden die Multi-Signatur-Wallets durch das Auslösen einer sog. *„Suicide Funktion“*, die eine Selbstlöschung des gesamten Vertrags einschließlich der Code-Bibliothek zur Folge hat, zum Stillstand gebracht.

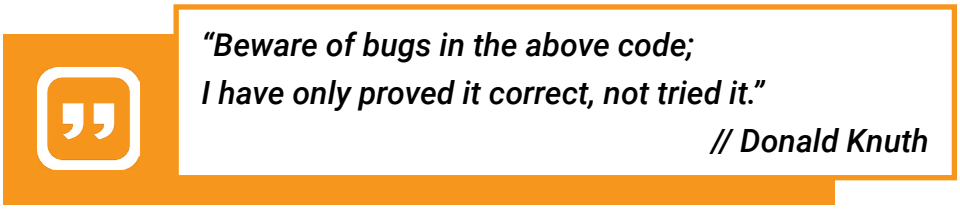
Multi-Signatur bezeichnet ein Feature, wodurch jede Transaktion durch mehrere Parteien bestätigt werden muss, also eine Signatur durch ihre jeweiligen privaten Schlüssel.

Auswirkungen

Kurz gesagt haben diverse Nutzer des Kryptogeldwallets Parity keinen Zugriff mehr auf ihr Krypto-Geld. Betroffen sind demnach alle Nutzer, die Multi-Signatur-Wallets verwenden, die nach dem 20. Juli erzeugt wurden. Laut dem Kryptowährungs-Experten Patrick McCorry handelt es sich dabei um schätzungsweise 600.000 Ether-Einheiten mit einem Wert von ca. 130 Millionen Euro. Dies entspricht ca. 1% aller bislang erzeugten Ethereum-Einheiten. Aktuell stuft Parity die Auswirkungen dieser Sicherheitslücke als kritisch ein. In Folge dessen fiel der Wert von Ethereum signifikant und erreicht damit seinen tiefsten Stand seit Wochen. Aus verschiedenen Quellen geht hervor, dass bislang kein Geld der eingefrorenen Ether-Einheiten gestohlen wurde, aber ein großer Betrag sei diesem Risiko ausgesetzt.

Problematik

Ein Nutzer mit dem Namen „*devops199*“, der diese Sicherheitslücke angeblich unbeabsichtigt ausgelöst haben soll, meldete den Vorfall auf der Plattform GitHub. Parity selbst will die Situation erst einmal analysieren und zu einem späteren Zeitpunkt weitere Details veröffentlichen. Zudem hat jeder Nutzer die Möglichkeit, auf der Webseite https://affected.parity.io/ zu prüfen, ob er von diesem Vorfall betroffen ist.



Ausblick

Aktuell arbeitet Parity an einer Lösung. Dennoch ist bislang unklar, ob und wie die Ether-Einheiten wieder freigegeben werden können. Einige Entwickler setzen sich für die Implementierung einer Verbesserung des Ethereum-Protokolls ein. Dies soll Ether-Besitzern ermöglichen, ihre Kryptowährung aus einem eingefrorenen Konto herauszulösen. Für diesen Vorgang wird allerdings ein „*Hard Fork*“ benötigt, welcher derzeit umstritten ist und Parity Technologies nachhaltig verletzen würde.

Ihr Vorteil

Mit der Vison, Zukunftsthemen wie beispielsweise die Blockchain nicht außer Acht zu lassen, haben Sie mit der mVISE einen Partner an Ihrer Seite, der sich stetig mit neuen Emerging Technologies auseinandersetzt. Wir bieten Ihnen zudem verschiedenste Lösungen aus den Bereichen Mobility, Virtualization und Security.

Wir begleiten Sie auf Ihrem Weg
in eine sichere Zukunft – Sprechen Sie uns an!

ÜBER DEN AUTOR

Bernhard Borsch ist seit 2014 für die mVISE AG tätig. Als Manager für das IT-Security Consulting beraten sein Team und er Kunden zum Thema IT-Security im Zuge der Herausforderungen der Digitalisierung. Zu seinen persönlichen Themenfeldern gehört neben den klassischen Themen, wie Enterprise- & Cloud-Security, PKI und Kryptographie, auch Zukunftsthemen der IT Security, wie Blockchain und Deception Technology. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

mVISE

Wir unterstützen mittelständische und große Unternehmen aller Branchen dabei, von der digitalen Revolution zu profitieren. Die besondere Kombination aus firmeneigenen Software-Lösungen mit ausgewählten Experten-Teams in den relevanten und aktuellen IT-Themengebieten schafft nachhaltige Wettbewerbsvorteile für unsere Kunden.

Unsere Experten bestimmen, gestalten, kreieren und steuern IT-Infrastrukturen und Software-Lösungen für Datenintegrations- und Enterprise-Data-Management-Projekte, mit dem Ziel, die aktuellen Geschäftsmodelle unserer Kunden zukunftssicher zu machen und gleichzeitig neue Geschäftsmodelle zu identifizieren.

Sprechen Sie uns an – gerne stellen wir Ihnen unser Angebot
in einem persönlichen Gespräch näher vor.
service@mvise.de | www.mvise.de

mVISE AG
Wahler Straße 2
40472 Düsseldorf
Fon: +49 211 78 17 80 – 0