"Beware of bugs in the above code;
I have only proved it correct, not tried it."
(Zitat Donald Knuth)

mVISE schaut hin: Parity Bug friert 130 Mio. 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 worden, nicht mehr transferiert werden können. Laut Experten handelt es sich dabei um Ether-Einheiten mit einem schätzungsweisen 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.

Wie kam es zu dem Vorfall?

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.

> Multi-Signatur bezeichnet das Feature, dass jede Transaktion aus einer Wallet durch mehrere Parteien bestätigt werden muss, also durch ihre jeweiligen privaten Schlüssel signiert wird.

Was zu dieser Zeit nicht bekannt war ist, 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.

Was sind die Auswirkungen?

Kurz gesagt haben diverse Nutzer des Kryptogeldwallet Parity keinen Zugriff mehr auf ihr Krypto-Geld. Betroffen sind demnach alle Nutzer, die Multi-Signatur-Wallets verwenden, die nach dem 20. Juli erzeugt worden. 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.

Wie wurde auf das Problem aufmerksam gemacht?

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.

Wie geht es weiter?

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.

Was bietet mVISE an?

Mit der Vison, Zukunftshemen wie bspw. 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.

Über den Autor

Bernhard Borsch ist seit zwei Jahren als Senior Consultant im Bereich Security für die mVISE AG tätig. Zu seinen Kernkompetenzen gehört neben PKI, Kryptographie und Mobile Security das Themenfeld Enterprise Security.

Derzeit unterstützt er mit seinem Team Kunden bei der Absicherung ihrer Enterprise Serverlandschaft. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

Bernhard Borsch
Senior Security Consultant bei der mVISE AG
Mail: Bernhard.Borsch@mvise.de
Mobil: +49 152 34151236