Sicherheitslücke bei Upgrade von Ethereum - ETH-Spin-off ChainSecurity stoppt Aktualisierung der Blockchain-Plattform in letzter Minute

Experten von ChainSecurity, dem Spin-off der ETH Zürich, haben eigenen Angaben nach "in letzter Minute" eine Sicherheitslücke bei einem geplanten Upgrade der Blockchain-Plattform Ethereum entdeckt. Am vergangenen Mittwoch hätte Ethereum eines seiner regelmässigen Upgrades erfahren sollen. Dieses wurde dank IT-Forscher Hubert Ritzdorf jedoch rechtzeitig gestoppt.

Verträge wären sonst angreifbar

Dem Fachmann ist aufgefallen, dass das Upgrade eine Sicherheitslücke öffnen würde. Er informierte das Ethereum-Kernteam, worauf dieses das Upgrade aussetzte. "Wäre das Upgrade wie geplant durchgeführt worden, hätten Nutzer mit Missbrauchsabsicht gewisse Verträge angreifen und so das Konto anderer Nutzer plündern können", erklärt Ritzdorf.

Konkret wäre die Sicherheitslücke entstanden, weil Ethereum den Preis, welche Nutzer für die Ausführung von smarten Verträgen bezahlen müssen, deutlich senken wollte. Dies geschah mit dem Ziel, die Benutzerfreundlichkeit zu erhöhen. Allerdings hätte diese Ã„nderung bewirkt, dass Nutzer mit Missbrauchsabsicht verschachtelte smarte Verträge hätten aufsetzen können, welche eine Transaktion im Hintergrund mehrmals statt nur einmal durchführen. Somit wäre es möglich gewesen, Ether-Konten anderer Nutzer zu plündern.

Erst vor wenigen Tagen entdeckt

Gegenwärtig verunmöglicht eine Kombination von höheren Vertragspreisen und eines Maximalbetrags pro Transaktion das Ausführen von versteckten smarten Verträgen im Hintergrund. Die aktuelle Sicherheitslücke hat Ritzdorf erst vor wenigen Tagen entdeckt, als er daran war, mögliche Auswirkungen des geplanten (und vorab im Detail veröffentlichten) Ethereum-Upgrades auf bestehende smarte Verträge von Firmenkunden auszumachen sowie die firmeneigenen Werkzeuge zur Sicherheitsprüfung zu aktualisieren.

"Smarte Verträge werden weder von Menschen ausgeführt noch von einem Computersystem, das von einer einzelnen Firma kontrolliert wird. Vielmehr werden sie von einer Art weltumspannenden Maschine ausgeführt. Dies schafft grosses Vertrauen punkto Sicherheit", so ChainSecurity-Co-Gründer Petar Tsankov. "Allerdings ist die Sicherheit nur dann hoch, wenn die Software und die einzelnen smarten Verträge keine Sicherheitslücken aufweisen. Dies zu überprüfen und unseren Kunden die Sicherheit zu garantieren, ist unser Geschäftsmodell."