KRYPTO NEWS
PART OF THE GLOBAL WOM NEWS NETWORK

Algo Stablecoin Protocol Beanstalk durch Governance Hijack abgeholzt

Ein Angreifer hat 24.830 Ether und 36 Millionen BEAN-Token im Wert von etwa 180 Millionen US-Dollar abgezogen Der Angreifer nutzte eine Lücke im Governance-Prozess des Protokolls aus, um einen böswilligen ȣVerbesserungsvorschlagȣ durchzusetzen. Beanstalk Farms, das als ȣein dezentrales kreditbasiertes Stablecoin-Protokollȣ bezeichnet wird, wurde am Sonntag für Papierverluste von etwa 180 Millionen Dollar ausgenutzt ج der letzte DeFi-Hack des Jahres. Damit ist es der fünftgrößte Protokoll-Exploit auf der Tracking-Site Rekt-Bestenliste und der zweitgrößte in diesem Jahr nach dem massiven Ronin-Bridge-Hack im März. Sicherheitsfirma PeckShield zuerst gemeldet die Nachrichten. Wie beim Ronin-Exploit bestehen die meisten gestohlenen Gelder aus Ether, die der Angreifer …

- Ein Angreifer hat 24.830 Ether und 36 Millionen BEAN-Token im Wert von etwa 180 Millionen US-Dollar abgezogen
- Der Angreifer nutzte eine Lücke im Governance-Prozess des Protokolls aus, um einen böswilligen ȣVerbesserungsvorschlagȣ durchzusetzen.

Beanstalk Farms, das als ȣein dezentrales kreditbasiertes Stablecoin-Protokollȣ bezeichnet wird, wurde am Sonntag für Papierverluste von etwa 180 Millionen Dollar ausgenutzt ȼ der letzte DeFi-Hack des Ɉahres.

Damit ist es der fünftgrößte Protokoll-Exploit auf der Tracking-Site Rekt-Bestenliste und der zweitgrößte in diesem Ɉahr nach dem massiven Ronin-Bridge-Hack im März. Sicherheitsfirma PeckShield zuerst gemeldet die Nachrichten.

Wie beim Ronin-Exploit bestehen die meisten gestohlenen Gelder aus Ether, die der Angreifer schnell in das Datenschutzprotokoll Tornado Cash einleitete, um die Herkunft der Token zu verschleiern.

Die Gruppe bestätigte den Exploit auf Twitter Sonntag und ist jetzt in Anbetracht ein Weg nach vorne.

Beanstalk hatte kürzlich einen Meilenstein gefeiert und 100 Millionen Dollar an geprägten BEAN-Token erreicht. Eine BEAN sollte einem US-Dollar entsprechen, aber im Gegensatz zu Stablecoins, die durch Fiat- oder Kryptosicherheiten gedeckt sind, verwendete Beanstalk ein neuartiges System finanzieller Anreize, um seine Bindung aufrechtzuerhalten, indem Kredite anstelle von Übersicherung verwendet wurden weißes Papier.

Das Protokoll wurde einem Audit des Blockchain-Sicherheitsexperten Omniscia unterzogen, aber die Firma gab in a an Post-Mortem-Analyse dass der Produktionscode, der von dem Exploit betroffen war, von dem abwich, was die Firma geprüft hatte.

Die Entwickler haben dieses Konto während eines Lives bestritten Bürgerversammlung Sonntag.

ȝWir sind nicht im Geschäft, mit dem Finger auf andere zu zeigen [but] Wir haben uns den von ihnen veröffentlichten Bericht angesehen und waren nicht der Meinung, dass es sich um einen echten Bericht über das handelt, was passiert istȝ, sagte der Hauptentwickler.

Omniscia wies auf einen ȝfür Flash-Kredite anfälligen Governance-Fehlerȝ als Schuldigen hin, der es dem Angreifer ermöglichte, einen böswilligen Governance-Vorschlag vorzuschlagen und dann durchzusetzen, der effektiv alle Vermögenswerte des Protokolls in die Brieftasche des Angreifers zurückzog.

Der Trick bestand darin, einen massiven Blitzkredit zu verwenden ج riesige Summen zu leihen, die innerhalb derselben Transaktion zurückgezahlt werden müssen ج und den üblichen Lebenszyklus eines Governance-Vorschlags zu umgehen. In ein bisschen DeFi-Magie unter Verwendung von geliehenen Stablecoins im Wert von 1,04 Milliarden US-Dollar erwarb der Angreifer kurzzeitig eine Supermehrheit der Stimmrechte des Protokolls, die darauf gerichtet war, bösartigen Code sofort auszuführen.

> ȝDas Beanstalk-Protokoll unterstützte Protokoll-Upgrades über seinen Beanstalk-Improvement-Proposal (BIP)-Governance-Mechanismus, und als solches war es möglich, dass ein Upgrade willkürlichen Code ausführte, wodurch der Angreifer seine gesperrten Gelder als Teil seines

> böswilligen Updates abrufen konnte. ঃ, schrieb Omniscia.

Es galt eine 24-stündige Wartezeit, aber der beleidigende BIP wurde als Angebot getarnt, Gelder zur Unterstützung der Ukraine zu spenden, und verstrich die Verzögerungszeit, bevor eine Abstimmung mit Supermehrheit wirksam werden würde.

ঃWir fanden es sehr seltsam, aber wir wussten offensichtlich nicht, was los war, welcher Angriff im Gange warঃ, erklärten die Entwickler während des Rathauses.

> ঃWir werden alles tun, um herauszufinden, wer das getan hat, und sie vor Gericht stellen.ঃ

Nach dem Exploit verloren die BEAN-Token des Protokolls sofort um 90 % an Wert und effektiv wurden alle anderen Vermögenswerte, einschließlich der vom Angreifer eingesetzten, liquidiert, was zu einem Nettogewinn von etwa 75 Millionen US-Dollar in Ether und anderen Token führte.

Laut PeckShield schickte der Hacker USDC im Wert von 250.000 USD an eine Adresse zur Unterstützung der Ukraine.

> 4/ Die anfänglichen Mittel zum Starten des Hacks werden abgezogen @SynapseProtocol und die meisten Ergebnisgewinne werden eingezahlt @TornadoCash. Derzeit verbleiben noch 15.154 ETH auf dem Konto des Hackers. Beachten Sie, dass der Hacker 250.000 USDC an die Ukraine Crypto Donation spendet. pic.twitter.com/jBjUJ0JbGj
>
> ج PeckShield Inc. (@peckshield) 17. April 2022

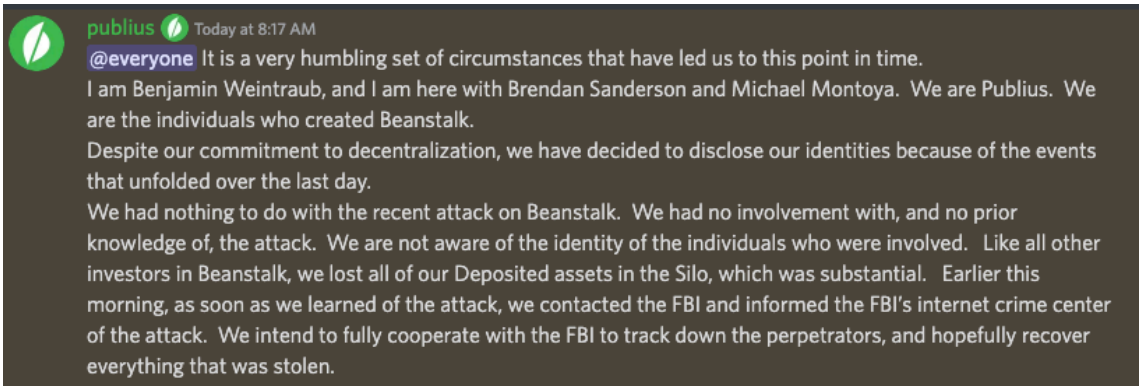
Samen der Hoffnung

Trotz der Katastrophe haben die Entwickler des Protokolls zugesagt, an dem Projekt weiterzuarbeiten.

> Heute ist ein schlechter Tag, aber es ist nicht das Ende. Wir waren überwältigt von der Unterstützung unserer Community an diesem Morgen. Der Weg nach vorne ist unklar, aber das Ziel war noch nie so klar.
>
> ج publius (@isthispublius) 17. April 2022

Während des Rathauses und so weiter den Discord der Gruppeunternahm das pseudonyme Team den außergewöhnlichen Schritt, ihre Identität preiszugeben und ihre Absicht zu erklären, mit den Strafverfolgungsbehörden zusammenzuarbeiten, in der Hoffnung, den Angreifer zu

identifizieren und Gelder zurückzufordern.



Dies ist nicht das erste Mal, dass Flash-Darlehen in einem DeFi-Exploit eingesetzt werden. Im vergangenen Jahr wurde Cream Finance um 130 Millionen Dollar geraubt. Das führte dazu, dass sein Governance-Token CREAM um 70 % einbrach ج von dem es sich nie wieder erholt hat.

Im Gegensatz zu anderen hochwertigen Hacks, wie dem Exploit der Solana-Wurmlochbrücke, verfügt Beanstalk nicht über Risikokapital, das möglicherweise eine Rettungsaktion zur Rekapitalisierung des Systems darstellen könnte.

Das Beanstalk-Team antwortete am Montag nicht sofort auf eine Bitte um Stellungnahme.

. .

Der Beitrag Algo Stablecoin Protocol Beanstalk Cut Down by Governance Hijack ist keine finanzielle Beratung.

Details

Besuchen Sie uns auf: krypto-news.at