Bitdefender

Hakerzy ukradli 1,6 miliona dolarów w aktywach kryptograficznych z bankomatów General Bytes Bitcoin

22.03.2023

Luka dnia zerowego w oprogramowaniu bankomatów General Bytes Bitcoin pozwoliła hakerom ukraść aktywa o wartości około 1,6 miliona dolarów. Zgodnie z informacją opublikowaną przez poszkodowaną firmę cyberprzestępcy podczas włamania wykorzystali exploit w głównym interfejsie usługi terminali, aby zdalnie przesłać złośliwą aplikację Java.

Chociaż firma nie podała dokładnej liczby aktywów kryptograficznych skradzionych przez cyberprzestępców, narzędzia do analizy łańcucha ujawniają, że zaginęło 56 283 BTC, 21 823 ETH i 1 219 183 LTC o łącznej wartości ponad 1,6 miliona dolarów.

Hakerzy ukradli 1,6 miliona dolarów – jak doszło do ataku?

Zgodnie z raportem zespołu do spraw cyberbezpieczeństwa firmy General Bytes hakerzy „przeskanowali przestrzeń adresową IP w chmurze Digital Ocean i zidentyfikowali działające usługi CAS w portach 7741, w tym usługę General Bytes Cloud i innych operatorów bankomatów GB obsługujących swoje serwery w Digital Ocean”.

Dzięki temu exploitowi cyberprzestępcy otrzymali między innymi pełny dostęp do bazy danych poszkodowanej firmy oraz możliwości:

- Odczytywania i odszyfrowywania gorących portfeli oraz wymiany kluczy API.
- Wyłączania uwierzytelniania dwuskładnikowego (2FA).
- Uzyskania poświadczenia użytkownika (nazwy użytkownika i jego hasła).
- Przelewania środków z gorących portfeli użytkowników.
- Dostępu do dzienników zdarzeń terminala.
- Dostępu do starych dzienników zawierających skanowanie prywatnych kluczy użytkowników.

„Wykorzystując tę lukę w zabezpieczeniach, hakerzy przesłali własną złośliwą aplikację bezpośrednio na serwer używany przez interfejs

administratora” – mówi pracownik General Bytes Bitcoin. – „Serwer aplikacji został domyślnie skonfigurowany do uruchamiania aplikacji w swoim folderze wdrażania”.

Kroki, które podjęła firma General Bytes Bitcoin

Chociaż firma twierdzi, że od 2021 roku przeprowadziła kilka audytów bezpieczeństwa, luka w zabezpieczeniach umknęła zespołowi zajmującemu się kryminalistyką cyfrową.

Ponadto raport sporządzony po ataku zawiera szczegółowe informacje, które pomogą operatorom ustalić, czy ich serwer został naruszony, a także szereg zaleceń dotyczących środków zaradczych. General Bytes wzywa wszystkich swoich operatorów do tego, aby:

- Zmienili wszystkie hasła swoich użytkowników.
- Unieważnili stare klucze API i wygenerowali nowe.
- Traktowali hasła CAS (krypto-bankomat) wszystkich użytkowników tak, jakby zostały naruszone.
- Korzystali z zapór ogniowych i sieci VPN, aby chronić CAS i terminale.

„Exploity typu Zero Day są często wykorzystywane przez cyberprzestępców. Hakerzy doskonale zdają sobie sprawę z tego, że

bardzo trudno podczas testów znaleźć wszystkie luki i większość nowych aplikacji zawiera wiele błędów, które mogą pozwolić na skuteczne włamanie do infrastruktury sieciowej danej firmy. Zasadniczo w momencie oddania aplikacji do użytku publicznego rozpoczyna się wyścig między hakerami i specjalistami do spraw cyberbezpieczeństwa o to, kto pierwszy znajdzie exploity" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/hakerzy-ukradli-16-miliona-dolarow/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 22.03.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.