Bitdefender

Hakerzy wykorzystują nową lukę w przeglądarce Chrome

22.12.2023

Google apeluje do użytkowników przeglądarki Chrome na komputerach stacjonarnych i urządzeniach mobilnych, aby wdrożyli poprawkę bezpieczeństwa dotyczącą luki, o której wiadomo, że jest wykorzystywana przez cyberprzestępców. Jak poinformował wczoraj gigant internetowy w swoim poradniku, przepełnienie bufora sterty w module komunikacji w czasie rzeczywistym przeglądarki Chrome zostało wykorzystane przez szkodliwe podmioty do atakowania bezbronnych użytkowników.

Nowa luka typu zero-day w przeglądarce Chrome

Błąd WebRTC, śledzony jako luka CVE-2023-7024, umożliwił ataki ukierunkowane w środowisku naturalnym. Fakt ten odkryli wcześniej Clément Lecigne i Vlad Stolyarov z grupy ds. analizy zagrożeń Google.

Haker zazwyczaj wykorzystuje takie luki w zabezpieczeniach, aby

wykraść poufne dane z urządzenia docelowego, a także, by uruchomić złośliwe oprogramowanie, które może przechwytywać naciśnięcia klawiszy, nagrywać wideo lub robić zdjęcia za pomocą kamer urządzenia, nagrywać dźwięk za pomocą wbudowanego mikrofonu itp.

„Google zdaje sobie sprawę, że w środowisku naturalnym istnieje exploit dla CVE-2023-7024” – czytamy w notatce.

Zespół Google TAG okresowo dokonuje takich ustaleń, ostatnio przypisując ataki sponsorowanym przez państwa autorytarnym podmiotom wdrażającym oprogramowanie szpiegowskie na podatnych na zagrożenia urządzeniach znanych osób.

Aktualizacja z tego tygodnia – dostępna dla wszystkich użytkowników komputerów stacjonarnych z systemami Windows, Mac i Linux, a także dla użytkowników Androida – skupia się wyłącznie na rozwiązaniu tej jednej słabości, dzięki czemu jest to awaryjna poprawka dla każdego, kto używa Chrome jako domyślnej przeglądarki internetowej.

W tym momencie luka nie ma wpływu na wersje przeglądarki Chrome na iPhone'a i iPada. Jednak Apple toczy własną walkę ze sponsorowanymi przez państwa hakerami, których celem są jego platformy, okresowo wydając poprawki systemu operacyjnego, aby załatać luki wykorzystywane przez operatorów oprogramowania szpiegującego.

Jak uchronić się przed lukami typu zero-day?

Jeśli używasz przeglądarki Chrome, zespół Bitdefender zaleca

zainstalowanie tej poprawki tak szybko, jak to możliwe. Na komputerze przejdź do Ustawienia -> Informacje o Chrome, pozwól przeglądarce pobrać aktualizację, a następnie zamknij i uruchom ponownie Chrome. Będziesz potrzebować wersji 120.0.6099.129 na Macu i Linuksie oraz 120.0.6099.129/130 na Windowsie.

Na Androidzie będziesz potrzebować wersji 120.0.6099.144. Wystarczy odwiedzić sklep Google Play, sprawdzić dostępność aktualizacji i pobrać nowo załataną przeglądarkę Chrome na swój smartfon.

„Ataki wykorzystujące exploity zero-day są zwykle ściśle ukierunkowane. Ogólna zasada ochrony przed nimi jest taka, że należy zachować ostrożność i dokonać aktualizacji tak szybko, jak to możliwe. Rozważ wdrożenie dedykowanego rozwiązania antywirusowego na wszystkich swoich urządzeniach osobistych, aby przez cały czas chronić się przed zagrożeniami internetowymi” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/hakerzy-wykorzystuja-nowa-luke-w-przegladarce-chrome/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 22.12.2023
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.