Bitdefender

Google ogłasza obsługę sandbox V8 w celu zwiększenia bezpieczeństwa użytkowników przeglądarki Chrome

11.04.2024

Firma Google ogłosiła obsługę V8 Sandbox, funkcji zabezpieczeń w przeglądarce Chrome, zaprojektowanej w celu łagodzenia problemów z uszkodzeniem pamięci JavaScript. Według oficjalnej strony tej funkcji zostanie ona zaimplementowana w przeglądarce Chrome 123; tę wersję należy uznać za „rodzaj wersji beta dla piaskownicy”.

Sandbox V8 – odpowiedź na problemy związane z silnikiem Javascript V8

W ciągu ostatnich kilku lat wykryto, że większość exploitów przeglądarki

Chrome powoduje problemy z uszkodzeniem pamięci w procesie wykorzystywanym do zdalnego wykonywania kodu (RCE). Około 60% tych problemów ma bezpośredni wpływ na silnik Javascript V8.

„Luki w zabezpieczeniach V8 rzadko są „klasycznymi" błędami powodującymi uszkodzenie pamięci (użycie po zwolnieniu, dostęp poza zakresem itp.). Zamiast tego są raczej subtelnymi problemami logicznymi, które z kolei można wykorzystać do uszkodzenia pamięci," – czytamy w ogłoszeniu v8.dev. „W związku z tym istniejące rozwiązania w zakresie bezpieczeństwa pamięci w większości nie mają zastosowania w wersji V8".

Izolowanie pamięci sterty V8 w celu ograniczenia luk w zabezpieczeniach

Badacze podkreślili, że większość luk w zabezpieczeniach V8 ma wspólną cechę: uszkodzenie pamięci często występuje w stercie V8. Dlatego badacze opracowali metodę segregacji pamięci sterty V8, aby powstrzymać rozprzestrzenianie się uszkodzeń pamięci do różnych obszarów pamięci procesu, a także złagodzić takie luki.

„Sandbox V8 musi zostać włączony w czasie kompilacji przy użyciu flagi v8_enable_sandbox" – czytamy w ogłoszeniu. „Nie jest (ze względów technicznych) możliwe włączenie sandboxu w czasie wykonywania. V8 Sandbox wymaga systemu 64-bitowego, ponieważ musi zarezerwować dużą ilość wirtualnej przestrzeni adresowej, obecnie jest to jeden terabajt.

Sandbox jest w stanie uśpienia od dwóch lat

Co więcej, ta funkcja jest dostępna od mniej więcej dwóch lat w 64-bitowych wersjach przeglądarki Chrome na systemy Windows, Linux, macOS, Android i ChromeOS. Pomimo tego, że aktualny sandbox nie jest w pełni funkcjonalny, decyzję o jego włączeniu podjęto, aby zapewnić brak problemów ze stabilnością i zebrać odpowiednie statystyki dotyczące wydajności.

Funkcja ta została uwzględniona w firmowym programie nagród za luki w zabezpieczeniach (VRP); łowcy nagród mogą wykazać się zdolnością do ominięcia mechanizmu, przestrzegając ścisłych, szczegółowych zasad składania wniosków.

„Rozwój Sandbox V8 jest niezwykle ważnym krokiem w zapewnieniu bezpieczeństwa użytkownikom przeglądarki Chrome. Uszkodzenia pamięci JavaSript niosą potencjalne ryzyko dla internautów, więc działania mające na celu zminimalizowanie tego problemu znacząco podniosą poziom cyberbezpieczeństwa w sieci” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/google-oglasza-obsluge-sandbox-v8/

Data udostępnienia: 11.04.2024

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.