Bitdefender

Luka Trojan Source naraża aplikacje na ukryte zatrucie

18.07.2024

Naukowcy z Uniwersytetu Cambridge, Nicholas Boucher i Ross Anderson, niedawno zidentyfikowali poważną lukę w zabezpieczeniach, która ma wpływ na sposób kompilacji kodu źródłowego. Luka, nazwana Trojan Source, może umożliwić atakującym wstrzykiwanie złośliwego kodu do aplikacji w sposób trudny do wykrycia podczas typowych przeglądów bezpieczeństwa.

Algorytm Unicode Bidi dotknięty nową luką Trojan Source

Nowa luka opiera się na manipulowaniu dwukierunkowym algorytmem Unicode (Bidi) w celu sprawienia, aby złośliwy kod wydawał się nieszkodliwy w kodzie źródłowym, ale zachowywał się inaczej po skompilowaniu.

Algorytm Bidi został zaprojektowany tak, aby uwzględniać teksty łączące języki pisane od lewej do prawej (LTR), takie jak angielski, z językami pisanymi od prawej do lewej (RTL), takimi jak arabski. Wykorzystując

lukę Trojan Source, osoby atakujące mogą zmieniać kolejność fragmentów tekstu, aby oszukać zarówno recenzentów, jak i zautomatyzowane narzędzia bezpieczeństwa.

Wada może maskować złośliwy kod jako nieszkodliwe fragmenty tekstu Może to prowadzić do ataków, w których istotne fragmenty kodu, takie jak kontrole bezpieczeństwa i procedury walidacji, są pomijane lub błędnie interpretowane jako nieszkodliwe komentarze. Na przykład to, co wydaje się nieszkodliwym kodem w przeglądzie bezpieczeństwa, może wywołać złośliwe operacje po skompilowaniu.

Chociaż problem ten stwarza bezpośrednie ryzyko dla przedsiębiorstw, implikacje dla codziennych użytkowników aplikacji oprogramowania są równie niepokojące. Dla użytkowników końcowych niebezpieczeństwo leży we wszechobecnej naturze aplikacji oprogramowania, które integrują kod z kilku źródeł, w tym bibliotek open source.

Zatruty kod może rozprzestrzeniać się niezauważenie

Jeśli sprawcy znajdą sposób na wstrzyknięcie kodu do powszechnie używanych bibliotek lub aplikacji za pomocą ataków typu upstream, zatruty kod może niezauważenie rozprzestrzenić się na szeroką gamę oprogramowania konsumenckiego, co może potencjalnie prowadzić do naruszenia danych osobowych, kradzieży pieniędzy i nieautoryzowanego dostępu do prywatnych systemów.

Wdrożono pewne środki łagodzące

Badacze zauważają, że platformy BitBucket i GitHub wdrożyły już pewne mechanizmy łagodzące lukę, w tym sprawdzanie składni i wyróżnianie użycia znaków Bidi. Jednak luka pozostaje szczególnie dotkliwa w powszechnie używanych językach skryptowych, takich jak SQL i Python. Językom tym często brakuje środków do wykrywania takich subtelności w manipulacji kodem, co czyni je bardziej podatnymi na ataki.

„Chociaż wdrożono pewne środki zaradcze, to nie są one wystarczająco kompleksowe, aby całkowicie wyeliminować ryzyko. Deweloperzy muszą zachować czujność, zwracając szczególną uwagę na fragmenty kodu importowane ze współdzielonych repozytoriów. Powinni pamiętać także o tym, aby zadbać o to, aby wszystkie zasoby były zabezpieczone za pomocą skutecznego systemu antywirusowego" – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/luka-trojan-source-naraza-aplikacje-na-ukryte-zatrucie/

Data udostępnienia: 18.07.2024
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.