Bitdefender

Haker oszukał badaczy cyberbezpieczeństwa za pomocą złośliwych dowodów koncepcji na GitHub

17.07.2023

Haker specjalizujący się w Linuksie zdołał oszukać badaczy cyberbezpieczeństwa i prawdopodobnie innych cyberprzestępców, używając fałszywych dowodów koncepcji (PoC), załadowanych złośliwym oprogramowaniem i opublikowanych na platformie kodowania GitHub. Exploit został wykryty podczas rutynowego skanowania przez firmę Uptycs zajmującą się analizą bezpieczeństwa, ujawniając sprytne wykorzystanie legalnych PoC w poszukiwaniu znanych luk w zabezpieczeniach wstrzykniętych przez złośliwe oprogramowanie do kradzieży haseł dla systemu Linux.

Haker oszukał badaczy cyberbezpieczeństwa – czym jest PoC?

PoC to kluczowe narzędzia w dziedzinie cyberbezpieczeństwa, umożliwiające naukowcom zrozumienie, przetestowanie i analizę potencjalnych skutków publicznie ujawnionych luk w zabezpieczeniach. Jednak ich wszechobecność może również dać cyberprzestępcom możliwość skuteczniejszego przeprowadzania ataków, jeśli zostaną wykorzystane do identyfikowania słabych punktów w atakowanych systemach.

W tym przypadku haker specjalizujący się w systemie Linux sklonował prawdziwe PoC w poszukiwaniu znanych luk w zabezpieczeniach, uzupełnił je złośliwym oprogramowaniem i ponownie przesłał do GitHub. Zanim Uptycs wykrył złośliwe działanie, jeden z fałszywych PoC został już sklonowany lub „rozwidlony” 25 razy, a drugi 20 razy.

Fałszywe PoC uruchamiały znaki ostrzegawcze podczas standardowego skanowania, wskazujące na nieprawidłowości, takie jak próby nieautoryzowanego dostępu do systemu, nietypowe transfery danych i nieoczekiwane połączenia sieciowe.

Jeden fałszywy PoC został zamaskowany jako rozwiązanie luki w zabezpieczeniach o wysokim poziomie ważności (CVSS: 7.0/10) typu use-after-free, znanej jako CVE-2023-35829, która wpływała na jądro Linuksa przed wersją 6.3.2. Fałszywy PoC zawierał dodatkowy plik: src/aclocal.m4, ukryty program do pobierania skryptów bash dla systemu Linux, którego nie ma w legalnej wersji. Skrypt został użyty do zebrania danych maszynowych, w tym nazwy hosta, nazwy użytkownika i zawartości katalogu domowego.

„Jego sposób działania jest dość przebiegły” – powiedział Uptycs w poradniku bezpieczeństwa. „Wykorzystywany do tworzenia plików wykonywalnych z plików kodu źródłowego, wykorzystuje polecenie make do tworzenia pliku kworker i dodaje swoją ścieżkę do pliku bashrc, umożliwiając w ten sposób złośliwemu oprogramowaniu ciągłe działanie w systemie ofiary”.

Użytkownik GitHub opublikował również inny złośliwy PoC, udając poprawkę dla CVE-2023-20871, luki w zabezpieczeniach o wysokim poziomie ważności (CVSS: 7.8/10) umożliwiającej eskalację uprawnień, która ma wpływ na hiperwizor VMware Fusion. Oba fałszywe PoC były prawie identyczne, poza ich nazwami.

W jaki sposób ochronić się przed takimi atakami?

Po wykryciu fałszywych PoC konto użytkownika GitHub zostało dezaktywowane, a złośliwa zawartość usunięta. Uptycs doradza osobom, które mogły użyć fałszywych PoC, usunięcie nieautoryzowanych kluczy SSH, sprawdzenie /tmp/.iCE-unix.pid, usunięcie kworkerpliku i ścieżki kworkerz bashrcpliku.

„Aby zapobiec rozprzestrzenianiu się takich infekcji, podczas pobierania nowych plików specjaliści do spraw cyberbezpieczeństwa powinni zawsze korzystać z sandboxów lub odizolowanego środowiska. W stale zmieniającym się świecie cyberbezpieczeństwa czujność i ostrożne praktyki są równie ważne, jak najbardziej wyrafinowane zabezpieczenia” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Haker oszukał badaczy cyberbezpieczeństwa za pomocą złośliwych dowodów koncepcji na GitHub

Źródło:https://bitdefender.pl/haker-oszukal-badaczy-cyberbezpieczenstwa/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 17.07.2023
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.