

Poważna podatność zdalnego wykonania kodu w sterowniku win32k.sys w Windows 7

Firma badawcza Secunia (na podstawie tweeta użytkownika w3bd3vil) poinformowała o wykryciu poważnej podatności w 64-bitowej edycji Windows 7. Przy pomocy zdalnego kodu możliwe jest (z pomocą przeglądarki Safari pracującej na takim systemie) spowodowanie zamazania części pamięci (i spowodowanie BSOD).

Na Twitterze użytkownik o identyfikatorze w3bd3vil opublikował odnośnik do snippetu HTML który powoduje BSOD na 64 bitowym Windows 7 (przy wejściu na niego przy użyciu przeglądarki Safari). Kluczową częścią tego kodu jest tag iframe z dużą wartością w atrybucie height. Jednak problem nie jest związany z przeglądarką a ze sterownikiem systemowym win32k.sys (funkcja NtGdiDrawStream). W związku z tym prawdopodobne jest, że wkrótce ujawnione zostaną inne wektory ataku (np. przy pomocy innych przeglądarek).

Brak póki co oficjalnej publikacji Microsoft w sprawie tej podatności.

[Zawieś w Windows 7 64bit \(IFRAME, 0day\)](#)

[Secunia Advisory SA47237 Microsoft Windows win32k.sys Memory Corruption Vulnerability](#)

ISC Diary: [New Vulnerability in Windows 7 64 bit](#)

Źródło: [Secunia](#)

[Idź na górę strony](#)