**Nie używasz Internet Explorera? Nadal możesz być narażony na ryzyko**

**Można by sądzić, że jakiekolwiek problemy z bezpieczeństwem, które stwarza Internet Explorer, nie powinny stanowić specjalnego zagrożenia. Przecież większość użytkowników komputerów przeniosła się do nowocześniejszych, alternatywnych przeglądarek, takich jak Chrome, Brave, Firefox, Safari lub Microsoft Edge.**

Nawet sam Microsoft ostrzegał firmy przed zagrożeniami, do jakich prowadzi ustawianie IE jako przeglądarki domyślnej, która nie jest już aktualizowana do obsługi nowych standardów sieciowych i może pozostawić użytkowników w „epoce lodowcowej”.

Są nawet tacy, którzy utrzymywali, że Microsoft powinien był zaprzestać wydawania poprawek bezpieczeństwa, do przestarzałego kodu IE, już cztery lata po pojawieniu się Edge’a, co wymusiłoby migrację użytkowników do nowej przeglądarki.

Cóż, gdyby potrzebny był inny argument dla pozbycia się IE, to analityk bezpieczeństwa John Page (znany na Twitterze jako @hyp3rlinx) właśnie go dostarcza.

Na swojej stronie opublikował on kod (z oczywistych powodów nie będziemy go tutaj przywoływać), który pokazuje, jak użytkownicy otwierający lokalnie plik-pułapkę z rozszerzeniem .MHT mogą bezwiednie udostępniać informacje zdalnemu napastnikowi.

Pliki .MHT (rozszerzenie oznacza archiwum internetowe) są domyślnym formatem, w jakim przeglądarka IE zapisuje strony internetowe.

Jeśli będziesz chciał otworzyć plik .MHT na komputerze z systemem Windows 7, Windows 10 lub Windows Server 2012 R2, to nastąpi próba załadowania go przez Internet Explorer, niezależnie od tego, jaka przeglądarka jest w systemie domyślna (IE 11 dostarczany jest klientom indywidualnym z każdą wersją systemu Windows, również Windows 10. W przypadku licencji edukacyjnej lub korporacyjnej, można ją opcjonalnie wyłączyć).

Page’owi udało się wykryć sposób wykorzystania exploita zero-day XXE (XML eXternal Entity) oparty na mechanizmie przetwarzania plików MHT przez Internet Explorer. Na swojej stronie napisał on: „Może to pozwolić atakującemu zdalnie na potencjalną eksfiltrację lokalnych plików i zdalne dotarcie do informacji o wersji lokalnie zainstalowanego programu”.

Analityk podaje przykład, jak opisana podatność może być wykorzystana do ujawnienia szczegółów dotyczących wersji zainstalowanego oprogramowania, które potencjalnie będą użyteczne przy próbie ataku na system.

Wszystko, co atakujący musiałby zrobić, to użyć inżynierii społecznej do nakłonienia ofiary do otwarcia złośliwego pliku .MHT.

Page poinformował Microsoft o problemie pod koniec marca, ale odpowiedź firmy sugeruje, że nie obiecują poprawki:

„*Ustaliliśmy, że poprawka dotycząca zgłoszonego problemu zostanie uwzględniona w przyszłej wersji tego produktu lub usługi. W tej chwili nie będziemy dostarczać bieżących aktualizacji związanych ze zgłoszonym błędem. Sprawa została zamknięta*”.

**Co więc należy robić?**

“*Jeżeli nie używamy oprogramowania antywirusowego, wskazane jest wyłączenie Internet Explorera w opcjach systemu Windows*” - radzą specjaliści Bitdefender z firmy Marken Systemy Antywirusowe.