**Dziura w bezpieczeństwie przeglądarki Safari firmy Apple**

**W trakcie badań nad różnymi rodzajami szkodliwych programów dla systemu OS X firmy Apple eksperci z Kaspersky Lab natknęli się na poważny błąd w bezpieczeństwie przeglądarki internetowej Safari.**

Problem związany jest z funkcją pozwalającą na przywrócenie stron otwartych w poprzedniej sesji i pozwala szkodliwemu użytkownikowi na odczytanie danych uwierzytelniania użytkowników.

Safari, podobnie jak wiele innych przeglądarek, wyposażone jest w funkcję przywracania poprzedniej sesji. Innymi słowy, wszystkie strony, które były otwarte w poprzedniej sesji przeglądarki – nawet te, które wymagają uwierzytelniania – mogą zostać ponownie otwarte w kilku prostych krokach. Czy jest to wygodne? Oczywiście – szczególnie, gdy przeglądarka zawiesi się lub gdy zamkniemy jej okno przez przypadek. Czy jednak jest to bezpieczne? Niestety nie.

Aby przeglądarka mogła wiedzieć, co było otwarte na końcu poprzedniej sesji, odpowiednie informacje muszą być gdzieś przechowywane. Oczywiście, dane takie powinny znajdować się w miejscu, które nie jest łatwo dostępne dla każdego i powinny być zaszyfrowane.

Safari jednak nie szyfruje tych informacji, a do tego przechowuje je w pliku LastSession.plist (jest to typowy format plików dla systemu OS X), który bez problemu każdy może otworzyć. W wyniku tego każdy może bez kłopotu przejrzeć dane użytkownika związane z uwierzytelnianiem.

W Safari dostępna jest funkcja „Otwórz wszystkie okna z ostatniej sesji”, która pozwala na odzyskanie stron aktywnych przed poprzednim zamknięciem przeglądarki – strony są otwierane w takim samym stanie, w jakim znajdowały się w poprzedniej sesji. To właśnie ta funkcja wykorzystuje dane z pliku LastSession.plist. Mechanizm ten jest dostępny w następujących wersjach Safari dla systemu OS X:

OS X 10.8.5, Safari 6.0.5 (8536.30.1),

OS X 10.7.5, Safari 6.0.5 (7536.30.1).

„*Nietrudno wyobrazić sobie konsekwencje powstania szkodliwego programu uzyskującego dostęp do pliku LastSession.plist w systemie, w którym użytkownik loguje się do Facebooka, Gmaila, Twittera, kont bankowych i innych serwisów online”* – mówi **Wiaczesław Zakorzewski**, ekspert z Kaspersky Lab. *„Naszym zdaniem przechowywanie takich danych w niezaszyfrowanym, ogólnie dostępnym pliku jest poważną luką w bezpieczeństwie, która daje cyberprzestępcom duże możliwości łatwego uzyskania danych uwierzytelniających użytkowników”.*

Eksperci z Kaspersky Lab poinformowali już firmę Apple o wykrytym problemie.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.