

MICROSOFT NAPRAWIŁ LUKĘ BEZPIECZEŃSTWA W OPROGRAMOWANIU TEAMS

Microsoft naprawił lukę bezpieczeństwa w oprogramowaniu Teams do obsługi współpracy zdalnej i rozmów firmowych. Podatność pozwalała cyberprzestępcom na wykorzystywanie plików w formacie .gif do przejmowania kont użytkowników i wykradania ich danych.

O istnieniu błędu koncern z Redmond poinformowała firma CyberArk z branży cyberbezpieczeństwa. Według ekspertów, potencjalni atakujący mogli poprzez wysłanie złośliwego pliku .gif użytkownikom Microsoft Teams przejąć ich tokeny uwierzytelniające dostęp do konta w programie. Jak podkreślili specjaliści, spreparowany przez hakerów plik .gif nie musi być nawet widoczny dla atakowanego użytkownika, przez co model działania cyberprzestępców jest tym groźniejszy - gdyż trudno wykrywalny.

Cytowana przez serwis Computer Weekly firma CyberArk zwraca uwagę, że hakerzy wykorzystujący tę metodę ataku mogli z łatwością prowadzić działania przeciwko każdemu użytkownikowi w ramach sieci, z której łączył się z aplikacją Microsoft Teams, a tym samym - wykradać poufne dane firmowe i przejmować konta wielu osób. Analizowany model ataku był również skuteczny w przypadku rozmów grupowych.

"Nawet, jeśli atakujący nie uzyskają dużo informacji z konta użytkownika na Teams, mogą użyć go do penetracji zespołu danej organizacji. Cyberprzestępcy mogą też dotrzeć do danych przechowywanych na kontach innych użytkowników Teams w ramach jednej sieci - nierzadko poufnych, często mających dużą wartość jako tajemnice handlowe czy plany biznesowe" - podkreśliła firma CyberArk.

Według ekspertów kolejnym ryzykiem związanym z istnieniem luki w programie Teams była możliwość wykorzystania jej do podszycia się pod szefostwo danej firmy i rozesłania pracownikom fałszywych informacji, bądź też wyłudzenia od nich danych.