**Zoom rozwiązał kolejny problem bezpieczeństwa. Firma współpracowała z izraelskimi ekspertami.**

**Problem bezpieczeństwa w funkcji dostosowywania adresu URL zagrażał użytkownikom Zoom – najpopularniejszej na świecie usługi telekonferencyjnej. Błąd w aplikacji mógł pozwolić hakerom do manipulowania linkami ID spotkania np. w celach phishingowych, pozwalają m.in. na wykradanie danych uwierzytelniających – informują eksperci Check Point Research.**

Błąd w funkcji „Vanity URLs” mógł pozwalać cyberprzestępcą na wysyłanie legalnie wyglądających zaproszeń na spotkania Zoom, będących w rzeczywistości środkiem do rozpowszechniania złośliwego oprogramowania oraz przejmowania danych uwierzytelniających – wskazują eksperci. To nie pierwsza luka, która mogła zagrażać popularnej usłudze Zoom. Na początku roku Check Point wsparł Zoom w naprawie innej podatności, pozwalającej hakerom na dołączanie do spotkań bez zaproszenia.

Popularność usługi Zoom znacząco wzrosła podczas epidemii COVID-19, gdy większość przedsiębiorstw przestawiło się na pracę zdalną. O ile w grudniu 2019 roku Zoom odnotowywał około 10 milionów uczestników spotkań dziennie, to w kwietniu 2020 roku było już ich ponad 300 milionów!

Rosnącą sukces usług wideokonferencyjnych od początku roku starają się wykorzystać cyberprzestępcy m.in. w kampaniach phishingowych. Wg Check Pointa szczególne wzrosty odnotowano w przypadku rejestracji złośliwych domen oraz instalacji programów podszywających się pod aplikacje Zoom.

Potencjalny problem z bezpieczeństwem „URL Vanity” został znaleziony przez badaczy w ramach wcześniejszej styczniowej współpracy. Mógł on pozwolić hakerom na próbę manipulowania niestandardowym adresem URL (np. <https://yourcompany.zoom.us>) na dwa sposoby:

**Prze targetowanie za pomocą linków bezpośrednich**: podczas konfigurowania spotkania haker może zmienić adres URL zaproszenia, aby uwzględnić wybraną przez siebie zarejestrowaną subdomenę. Innymi słowy, jeśli oryginalny odsyłacz to <https://zoom.us/j/##########>, osoba atakująca może zmienić go na [https://<nazwa](https://%3cnazwa) organizacji>.zoom.us/j/##########. Bez specjalnego szkolenia z zakresu cyberbezpieczeństwa dotyczącego rozpoznawania odpowiedniego adresu URL użytkownik otrzymujący to zaproszenie może nie rozpoznać, że zaproszenie nie było autentyczne lub wysłane przez rzeczywistą lub prawdziwą organizację.

l **Targetowanie na dedykowane interfejsy internetowe Zoom:** niektóre organizacje mają własny interfejs sieciowy Zoom do obsługi konferencji. Haker może zaatakować taki interfejs i podjąć próbę przekierowania użytkownika do wprowadzenia identyfikatora spotkania do złośliwego adresu „URL Vanity” zamiast do prawdziwego interfejsu internetowego Zoom. Podobnie jak w przypadku ataków na linki bezpośrednie, bez dokładnego przeszkolenia w zakresie cyberbezpieczeństwa ofiara takich ataków mogła nie być w stanie rozpoznać złośliwego adresu URL i paść ofiarą ataku.

Korzystając z obu metod, haker może próbować podszywać się pod pracownika organizacji i starać się pozyskać od ofiary dane uwierzytelniające lub poufne informacje.

*- Ponieważ Zoom stał się jednym z wiodących kanałów komunikacji na świecie dla firm, rządów i konsumentów, niezwykle ważne jest, aby uniemożliwić podmiotom zagrażającym wykorzystywanie Zoom do celów przestępczych.* – stwierdził Adi Ikan, kierownik grupy ds. Badań i ochrony sieci w Check Point - *Współpracując z zespołem bezpieczeństwa Zoom, pomogliśmy zapewnić użytkownikom na całym świecie bezpieczniejszą, prostszą i godną zaufaną komunikację, aby mogli w pełni korzystać z zalet tej usługi.*

Jak zapewniają obie firmy, załatanie potencjalnych podatności było wspólnym wysiłkiem Zooma oraz ekspertów cyberbezpieczeństwa z Check Pointa. - *Wspólnie podjęliśmy ważne kroki, aby chronić użytkowników Zoom na całym świecie* - dodał Adi Ikan.

Symulacja ataku została zaprezentowana pod linkiem: <https://youtu.be/YIrgDkVYLKU>

Pełna analiza podatności omówiona jest na stronie: <https://blog.checkpoint.com/2020/07/16/fixing-the-zoom-vanity-clause-check-point-and-zoom-collaborate-to-fix-vanity-url-issue/>