aut. Małgorzata Fraser 14.07.2021

KOLEJNE PROBLEMY SOLARWINDS. CYBERPRZESTĘPCY AKTYWNIE WYKORZYSTUJĄ PODATNOŚĆ ZERO DAY

Firma SolarWinds poinformowała o kolejnej luce bezpieczeństwa typu *zero day* w swoim oprogramowaniu po tym, jak ostrzegł przed nią koncern Microsoft. Co gorsza – luka jest aktywnie wykorzystywana przez cyberprzestępców, których działalność - według ekspertów - ma być związana z Chinami.

Podatność zlokalizowana jest w usługach z linii Serv-U i stwarza zagrożenie dla komercyjnych VPN-ów SolarWinds oraz innych produktów konsumenckich, takich jak routery.

Microsoft poinformował, że zlokalizowana w produktach SolarWinds luka jest obecnie **aktywnie wykorzystywana przez cybeprzestępców powiązanych z Chinami.** Grupa identyfikuje się jako DEV-0322, a według firmy z Redmond w swoich działaniach bardzo często posługuje się botnetami złożonymi z urządzeń Internetu Rzeczy i routerów.

DEV-0322 to gang cyberprzestępczy, który jest szczególnie aktywny w atakach na sektor obronności USA i firmy zajmujące się rozwojem oprogramowania dla biznesu.

Możliwe zainstalowanie złośliwego oprogramowania

Podatność *zero day* wykryta w produktach SolarWinds identyfikowana jest jako CVE-2021-35211. Produkty Serv-U, w których jest zlokalizowana, **wykorzystywane są do transferu plików w ramach sieci.** Podczas połączenia z internetem, protokół SSH umożliwia cyberprzestępcom zdalne wykonanie złośliwego kodu oraz pozyskanie wysokich uprawnień dostępowych w ramach atakowanej sieci.

Dzięki takiemu wykorzystaniu luki, cyberprzestępcy zyskują łatwy dostęp do **możliwości instalacji dowolnego złośliwego oprogramowania na komputerach atakowanej sieci, a także wglądu i modyfikacji przetwarzanych w niej danych.**

W grudniu ubiegłego roku produkty firmy SolarWinds zostały wykorzystane przez cyberprzestępców do jednego z największych cyberataków w historii.

Zainfekowano wówczas około 18 tys. firm, organizacji i instytucji korzystających z oprogramowania do zarządzania Orion. **Wśród nich znalazły się organy administracji publicznej m.in. z USA, ale i z Polski.** Grudniowy cyberatak został przez Stany Zjednoczone przypisany wywiadowi zagranicznemu Federacji Rosyjskiej.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.