Cyberdefence 24

aut. Szymon Palczewski 06.08.2020

INFRASTRUKTURA ENERGETYCZNA Z KRYTYCZNYMI LUKAMI. GROZI NAM BLACKOUT?

Luki w najmniejszych komponentach infrastruktury przemysłowej i energetycznej mogą doprowadzić do incydentów paraliżujących działalność całego zakładu lub przedsiębiorstwa. Są one często pomijane w przeglądach bezpieczeństwa, a ich podatność ma kluczowe znaczenie dla ochrony przed cyberatakami. Czy tego typu luki zostały wykorzystane przez rosyjskich hakerów podczas kampanii wymierzonej w ukraiński sektor energetyczny w 2015 roku?

Bramy protokołów (ang. *protocol gateways*) odgrywają istotną rolę w sieciach przemysłowych, ponieważ zapewniają sprawne funkcjonowanie urządzeń i ich wzajemne połączenie. Dzięki temu różne elementy infrastruktury, w tym czujniki, maszyny czy komputery, mogą przesyłać między sobą dane dla utrzymania efektywności procesu przemysłowego.

Specjaliści Trend Micro zidentyfikowali podatności w bramach protokołów, które mają istotne znaczenie dla bezpieczeństwa infrastruktury. „Oceniliśmy i przetestowaliśmy różne bramy protokołów, aby zobaczyć, w jaki sposób złośliwy aktor może wykorzystać luki (...) do przeprowadzania trudnych do wykrycia ataków na obiekty przemysłowe" – wskazują eksperci firmy. Badanie dotyczyło przede wszystkim dostawców z Francji, Tajwanu i Stanów Zjednoczonych.

Według analiz, podatności umożliwiają podmiotom zewnętrznym rozsyłanie zainfekowanych ładunków w celu wywołania niepożądanych zakłóceń, minimalizując ryzyko wykrycia. Powiązania między różnymi elementami infrastruktury sprawiają, że złośliwe oprogramowanie może z łatwością przenikać do kolejnych komponentów. W związku z tym kampanie wymierzone w bramy protokołów są trudniejsze do wykrycia. „Ponadto wbudowane urządzenia sieciowe są trudne do monitorowania i kontroli, co daje zewnętrznemu podmiotowi szerszy margines ataku" – podkreślają specjaliści.

W raporcie „Lost in Translation: When Industrial Protocol Translation Goes Wrong", opracowanym przez Trend Micro, wyszczególniono konkretne „problemy i luki" w zabezpieczeniach, jakie udało się zidentyfikować podczas badań. Po pierwsze, słaba jakość szyfrowania, co umożliwia łatwiejsze odkodowanie konfiguracji baz danych, a także nieodpowiednie wdrożenie mechanizmów poufności, które może skutkować ujawnieniem wrażliwych informacji. Po drugie, często występują luki w uwierzytelnianiu przez co rośnie ryzyko nieautoryzowanego dostępu oraz kampanii DDoS (odmowa dostępu). „I co najważniejsze, konkretne scenariusze, w których osoba atakująca może wykorzystać luki, aby wydać polecenia, które mogą sabotować proces operacyjny" – czytamy w raporcie.

Wskazane podatności mogą znacząco wpłynąć na bezpieczeństwo obiektu, procesy i wydajność. Dają złośliwym aktorom podstawę do prowadzenia kampanii w celu sparaliżowania konkretnych urządzeń czy też kontroli i obserwacji działalności zakładów przemysłowych dla gromadzenia danych. „Ta utrata kontroli może spowodować, że docelowy zakład nie będzie w stanie dostarczyć niezbędnych produktów, takich jak energia i woda lub wpłynąć na jakość i bezpieczeństwo produktów fabryki" – stwierdzono w analizie.

Wykryte luki mogły być wykorzystane przez złośliwych aktorów do przeprowadzenia kampanii wymierzonych na przykład w sektor energetyczny, tak jak to miało miejsce w 2015 roku na Ukrainie. Wówczas rosyjscy hakerzy włamali się do lokalnych firm energetycznych, instalując ładunek na kluczowym sprzęcie w podstacjach elektroenergetycznych. Ich działalność doprowadziła do blackoutu.

Raport Trend Micro ma zachęcić podmioty przemysłowe i sektora energetycznego do prowadzenia szczegółowej analizy nawet najmniejszych i pozornie nieistotnych urządzeń, ponieważ mogą one mieć krytyczne znaczenie dla bezpieczeństwa. To samo dotyczy bram protokołów. „Te urządzenia bywają pomijane" – podkreślił Marco Balduzzi z Trend Micro, cytowany przez serwis CyberScoop. – „Niektórzy dostawcy zwracają uwagę na bezpieczeństwo, a inni nie".

W wyniku odkrycia podatności część wadliwych komponentów została wycofana przez dostawców. Przykładem może być firma Nexcom z Tajwanu, która poinformowała, że jej produkt nie trafi już na rynek. W zamian przedsiębiorstwo wypuściło nowy, bezpieczniejszy model.

Daniel dos Santos, ekspert w Forescout Technologies, podkreślił, że do tej pory bramy protokołów nie zostały poddane wystarczającej kontroli bezpieczeństwa w branży przemysłowej i energetycznej. „Wszyscy muszą być świadomi wszelkich zasobów w sieci, a nie tylko tych, które uważamy za najbardziej krytyczne" – zaznaczył na łamach CyberScoop.