**Check Point ostrzega przed dziurami w systemach zabezpieczeń dostawców Internetu**

**Check Point® Software Technologies Ltd. (Nasdaq: CHKP), światowy lider w dziedzinie bezpieczeństwa Internetu, opublikował wyniki badań nad protokołem CPE WAN Management Protocol (CWMP/TR-069), wykorzystywanym przez największych dostawców Internetu (Internet Service Provider - ISP) na całym świecie do sterowania domowymi urządzeniami sieciowymi takimi jak routery Wi-Fi, telefony VoIP i wiele innych.**

Analitycy z oddziału Check Point’s Malware and Vulnerability Research Group, odkryli klika braków zabezpieczeń typu zero-day, które można wykorzystać do uzyskania nieautoryzowanego dostępu do milionów sieci domowych i firmowych. Dotyczy to błędów w zabezpieczeniu serwerów TR-069. Uzyskanie nieupoważnionego dostępu może doprowadzić do infekcji złośliwym oprogramowaniem na szeroką skalę, nielegalnej inwigilacji i ingerencji w prywatność oraz zakłócenia działania usług, w tym wyłączenie Internetu dostarczanego przez danego ISP. Co więcej, atakujący hakerzy mogą wykraść dane osobowe i finansowe licznych klientów indywidualnych i biznesowych.

Bardziej szczegółowe analizy wykryły niepokojącą liczbę niezabezpieczonych ISP, narażonych na nieautoryzowane zdalne przejęcie kontroli. Check Point poinformował wspomnianych dostawców i udzielił im pomocy w usunięciu wszystkich podatności.

Kluczowe wnioski:

W przypadku niewykrycia problemu, potencjalny atakujący mógłby przejąć kontrolę nad milionami urządzeń sieciowych na całym świecie, co dałoby mu możliwość kradzieży danych finansowych i osobowych klientów biznesowych i indywidualnych.

Wiele implementacji TR-069 posiada liczne błędy w zabezpieczeniach. Check Point apeluje do wszystkich ISP oraz innych dostawców korzystających z protokołu do natychmiastowego sprawdzenia jakości bezpieczeństwa.

Klienci firmy Check Point posiadający Intrusion Prevention System (IPS) Software Blade zostali automatycznie zabezpieczeni przed opisanymi zagrożeniami.

“Główną misją firmy Check Point jest być o krok przed hakerami. Odkryte wady w implementacjach TR-069 mogły prowadzić do katastroficznych w skutkach atakach na dostawców Internetu i ich klientów na całym świecie. Działania naszego zespołu Malware and Vulnerability Research Group wciąż koncentrują się na wykrywaniu podobnych podatności i tworzeniu niezbędnej ochrony dostarczanej w czasie rzeczywistym – wszystko po to, by Internet mógł być bezpieczny”, mówi Shahar Tal, kierownik zespołu ds. badań nad podatnościami w firmie Check Point Point Software Technologies.

Grupa Malware and Vulnerability Research Group firmy Check Point regularnie przeprowadza testy najpopularniejszych programów w celu zapewnienia bezpieczeństwa Internetu na całym świecie. Aby uzyskać więcej informacji na temat innych badań i raportów, odwiedź:

<http://www.checkpoint.com/threatcloud-central/>.

​Check Point Software Technologies Ltd., światowy lider w dziedzinie bezpieczeństwa Internetu, opublikował wyniki badań nad protokołem CPE WAN Management Protocol, wykorzystywanym przez największych dostawców Internetu na całym świecie do sterowania domowymi urządzeniami sieciowymi.

W Polsce dystrybutorami produktów Check Point są firmy Clico Sp. z o.o. ([www.clico.pl](http://www.clico.pl/)) oraz RRC Poland Sp. z o.o. ([www.rrc.pl](http://www.rrc.pl/)).