[TLP: WHITE]
Krytyczna podatność CVE-2020-1350

Zespół CERT Polska rekomenduje administratorom systemów Windows Server, w każdej jego wersji, niezwłocznie zaaplikować poprawkę naprawiającą krytyczną podatność CVE-2020-1350 (CVSS 10/10).

Podatność

Podatność w usłudze DNS systemów Windows Server polega na błędnym mechanizmie parsowania odpowiedzi z rekordami DNS. Odpowiednio spreparowany rekord DNS może spowodować nadpisanie pamięci procesu z usługą DNS.

Skutki

Pomyślne wykorzystanie podatności pozwala atakującemu na wykonanie kodu w systemie z uprawnieniami użytkownika *Local System*. Powoduje to, że atakujący łatwo może uzyskać kontrolę nad całym systemem. Często ten sam serwer jest również kontrolerem domeny, co będzie wiązać się z uzyskaniem przez atakującego praw administratora domeny.

W momencie wydania tego dokumentu (14.07.2020 godz. 22:00) nie jest znany publicznie dostępny exploit wykorzystujący tę podatność, jednak należy spodziewać się, że może się on pojawić już nawet w ciągu kilkunastu następnych godzin lub kilku dni. Potencjalny exploit, jak zaznacza sama firma Microsoft, może mieć charakter samorozprzestrzeniającego się robaka.

Wektor ataku

Do przeprowadzenia ataku wystarczy, aby podatny serwer spróbował rozwiązać nazwę domenową z odpowiednio spreparowanym przez atakującego rekordem DNS. O rozwiązanie złośliwej nazwy domenowej „poprosić” może dowolna z usług działających na serwerze (np. serwer WWW) albo dowolny z komputerów w organizacji, który jako serwer DNS ustawiony ma podatny serwer. Obecny stan wiedzy nie pozwala jeszcze wykluczyć, że przykładowym wektorem ataku może być nie tylko uruchomienie złośliwej aplikacji na jednym z komputerów w organizacji, ale – choć jest to mało prawdopodobne – nawet otworzenie przygotowanej przez atakującego strony internetowej.

Poprawka i więcej informacji

Advisory firmy Microsoft z dostępną poprawką do pobrania oraz możliwym tymczasowym obejściem podatności poprzez modyfikację odpowiedniego klucza rejestru Windows: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350.

Dokładny, techniczny opis podatności jej znalazców: https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/.