CSIRT GOV

http://csirt.gov.pl/cer/wiadomosci/zagrozenia-i-podatnosc/723,Informacja-CERTGOVPL-w-zwiazku-z-zagrozeniem-quotSandWormquot.html
2018-10-16, 01:05

Informacja CERT.GOV.PL w związku z zagrożeniem "SandWorm"

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL informuje o nowym zagrożeniu, które zostało określone jako kampania cyberszpiegowska „SandWorm”.

Wykryta przez firmę iSight we współpracy z firmą Microsoft podatność typu 0-day (luka dotyczy wszystkich aktualnie wspieranych przez Microsoft systemów operacyjnych z rodziny Windows oraz Windows Server 2008 i 2012), była wykorzystywana przez grupę "SandWorm" do kampanii cyberszpiegowskiej wymierzonej w NATO, Unię Europejską, ukraińskie oraz zachodnioeuropejskie instytucje administracji publicznej, firmy z sektora energetycznego oraz telekomunikacyjnego, a także uczelnie w Stanach Zjednoczonych.

Atakujący do infekcji wykorzystali szereg podatności m.in. CVE-2010-3333, CVE-2012-0158, CVE-2013-3906, CVE-2014-1761 oraz ostatnio odkrytą CVE-2014-4114.
W dniu 14-10-2014r, firma Microsoft udostępniła łatkę na błąd CVE-2014-4114, który dotyczył luki występującej w mechanizmie Windows OLE. Poprawka usunęła możliwość zdalnego wykonywania kodu poprzez uruchomienie specjalnie spreparowanego pliku Microsoft Office, który zawiera obiekt OLE. Wykorzystanie przedmiotowej podatności pozwala na wykonanie kodu w kontekście aktualnie zalogowanego użytkownika. W przypadku, gdy zalogowany użytkownik posiadał prawa administratora atakujący mógł instalować programy, edytować lub kasować dane, a także tworzyć nowe konta z pełnymi uprawnieniami.

W związku z przedmiotowym zagrożeniem Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL podjął działania informacyjne skierowane do sektora energetycznego oraz instytucji administracji państwowej, zmierzające do ograniczenia możliwości eskalacji zagrożenia w sieciach i systemach dotkniętych cyberkampanią.

Zespół CERT.GOV.PL zaleca natychmiastową aktualizację systemów operacyjnych z rodziny Windows podatnych na przedmiotowy błąd. Więcej informacji o aktualizacji łatającej podatność można znaleźć w biuletynie bezpieczeństwa MS14-060 z dnia 14.10.2014 roku, który jest dostępny pod adresem https://technet.microsoft.com/library/security/ms14-060.

Dodatkowo CERT.GOV.PL informuje, że pod adresem http://www.isightpartners.com/2014/10/cve-2014-4114/ można uzyskać więcej informacji dotyczących przedmiotowego zagrożenia.