KRYTYCZNE AKTUALIZACJE – MICROSOFT, MOZILLA, VMWARE I WORDPRESS

Firmy Microsoft, Mozilla, VMware i Wordpress opublikowały poprawki dotyczące bezpieczeństwa swoich aplikacji. Zostały one zakwalifikowane jako „ważne" lub „krytyczne" i dlatego należy je niezwłocznie zainstalować – apelują eksperci z Rządowego Zespołu Reagowania na Incydenty Komputerowe, który działa jako CERT.GOV.PL w Agencji Bezpieczeństwa Wewnętrznego.

Ponad 16 krytycznych aktualizacji firmy Microsoft oraz 11 ważnych zostało opublikowanych kanałem aktualizacji bezpieczeństwa. Rewizja dotyczy systemu operacyjnego Microsoft Windows w wersji desktopowej oraz serwerowej. Wersje które dostały poprawki Vista oraz nowsze na komputerach osobistych, dla wersji serwerowych są to wersje Windows Server 2008 oraz nowsze. Zastosowanie większości aktualizacji może wymagać restartu systemu, na którym zostały przeprowadzone zmiany.

Programy dla których aktualizacje wypuściła firma Mozilla to Firefox, Firefox ESR oraz Network Security Services (NSS). W przypadku wersji ESR – przeglądarki przeznaczonej dla dużych firm - większość aktualizacji ma oznaczenie ważne, a 2 elementy dostały oznaczenie krytyczne. Podobnie jest w wersji dla odbiorców prywatnych, jednak oprócz luk obecnych w wersji ESR pojawiają się mniej znaczące luki o znaczeniu średnim oraz niskim. Luka w bibliotece NSS posiada oznaczenie średnie. Podatności wykryte w poprzednich wersjach oprogramowania mogą umożliwić osobie atakującej przejęcie kontroli nad systemem.

W biuletynie firmy VMware znajdziemy aktualizacje podatności dotyczących oprogramowania vCenter Server, VMware NSX i vCNS oraz VMware vRealize Log. Wszystkie aktualizacje dostały oznaczenie co najmniej ważne, kilka z nich jest uznawane przez firmę jako luki o charakterze krytycznym, które wymagają natychmiastowej aktualizacji. Luki wykryte w poprzednich wersjach oprogramowania mogą umożliwić osobie atakującej m.in. na przejęcie kontroli nad podatnym systemem.

Nową aktualizację udostępniła także firma Wordpress. W nowej wersji 4.5.3 zostało poprawione wiele aspektów bezpieczeństwa, które według firmy powinny zostać nowelizowane jak najszybciej. Usunięto z niej dwa poważne błędy wykorzystujące XSS (Cross-site scripting) jako atak na stronę www. XSS to technika polegająca na umieszczeniu na serwisie WWW dodatkowego skryptu, który odpala się innym użytkowników po wejściu na zainfekowaną stronę. Wykorzystanie wykrytych błędów może umożliwić osobie atakującej przejęcie kontroli nad podatnym systemem.

Linki do wszystkich aktualizacji i biuletynów bezpieczeństwa są dostępne na stronie internetowej CERT.GOV.PL, który działa w strukturze Departamentu Bezpieczeństwa Teleinformatycznego ABW.

Zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni RP, w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego zespołu CERT w odniesieniu do administracji rządowej i sfery cywilnej. Podstawowym jego zadaniem jest zapewnianie i rozwijanie zdolności jednostek

organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami.

Realizuje on jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze cyberprzestrzeni RP(CRP). Stanowi drugi poziom Krajowego Systemu Reagowania na Incydenty Komputerowe.

Czytaj też: Nowa recepta na cyberataki wymierzone w firmy