CERT.GOV.PL: KRYTYCZNE AKTUALIZACJE – ADOBE, APPLE, CISCO I VMWARE

Firmy Adobe, Apple, Cisco i VMware opublikowały poprawki dotyczące bezpieczeństwa swych 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.

Firma Adobe w ramach opublikowanego niedawno biuletyny bezpieczeństwa zaktualizowała swoją aplikację ColdFusion w wersji 10 oraz 11, dostępną na platformach desktopowych. Aktualizacje posiadają odpowiednio wersję 21 oraz 10 dla starszej oraz nowszej wersji produktu firmy. Luka o oznaczeniu CVE-2016-4264 mogła zostać wykorzystane przez niepowołane osoby w celu pobrania informacji wrażliwych oraz poufnych z komputera ofiary. Lukę dla firmy Adobe odnalazł Dawid Golunski z grupy legalhacker.com i współpracował z firmą w celu jej zlikwidowania. Producent oprogramowania zaleca jak najszybszą aktualizacje swojego programu, hotfix jest już dostępny do pobrania za pomocą łącza internetowego.

Firma Apple zaktualizowała swój system przeznaczony na urządzenia mobilne klasy iPhone. Zaktualizowana luki zostały odkryte przez Citizen Lab oraz Lookout, posiadają odpowiednie oznaczenia od CVE-2016-4655 do CVE-2016-4657. Dwie z nich dotyczyły podatności występujących w jądrze systemu, które pozwalały na dostęp do wewnętrznej pamięci urządzenia oraz wykonania na nim operacji z poziomu konta administratora. Ostatnia z luk polegała na podatności wtyczki WebKit, która uaktywniła się po przejściu na stronę zarażoną wirusem.

W przypadku firmy Cisco zostały zaktualizowane w ramach comiesięcznego cyklu urządzenia odpowiedzialne za zarządzeni oraz obsługę sieci teleinformatycznych. Wśród nich:

- Cisco Firepower Management Center
- Cisco Application Policy Infrastructure Controller Enterprise Module
- Cisco Aironet 1800, 2800, and 3800 Series Access Point Platforms
- Cisco Adaptive Security Appliance
- Cisco IP Phone 8800 Series

- Cisco Identity Services Engine Admin Dashboard Page
- Cisco Smart Call Home Transport Gateway
- Cisco Unified Communications Manager
- Cisco WebEx Meetings Server

Wykryte luki mogą umożliwić zdalnej osobie atakującej na przejęcie kontroli nad podatnym systemem. Dlatego producent zaleca jak najszybszą aktualizację wszystkich urządzeń dotkniętych zagrożeniem hakerskim. Większość aktualizacji dostała oznaczenie krytyczne.

Oprócz tego w ramach aktualizacji swoich produktów firma VMware przeprowadziła rewizję swoich rozwiązań o nazwach VMware Identity Manager oraz vRealize Automation. Luki o oznaczeniach CVE-2016-5335, CVE-2016-5336 zostały oznaczone jako ważne dla bezpieczeństwa systemu, dlatego producent zaleca ich natychmiastową aktualizacje. Firma jednocześnie wraz z wprowadzonymi poprawkami zaktualizowała funkcjonalność samego oprogramowania.

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 poziom II-gi Krajowego Systemu Reagowania na Incydenty Komputerowe w CRP.