GOV CERT MAGYARORSZÁG
Nemzetbiztonsági Szakszolgálat
Kormányzati
Eseménykezelő Központ

Nemzetbiztonsági Szakszolgálat
Kormányzati Eseménykezelő Központ

Tájékoztató Hírlevél

A Kormányzati Eseménykezelő Központ a 2014.09.25-én a „BASH" kritikus sérülékenységgel kapcsolatban kiadott riasztását az alábbi információkkal egészíti ki.

A GNU Bash shell két könnyen kihasználható, kritikus sérülékenységére derült fény, mely a Linux és a Mac OS X alapú számítógépeket, illetve eszközöket is érinti.
A többszörös sebezhetőséget a Bash parancsfeldolgozása tartalmazza, amely nem megfelelően kezeli a környezeti változók és a függvények kapcsolatát. Ezek miatt, a *CVE-2014-6271* számú sérülékenységet kihasználva tetszőleges kódok válhatnak lefuttathatóvá, és akár CGI scriptekkel történő visszaélésekre is lehetőséget adhat, továbbá a *CVE-2014-7169* számú sérülékenységet kihasználva a távoli felhasználók fájlokat hozhatnak létre vagy írhatnak felül. A javított verzió telepítése után minden érzékeny információt meg kell vizsgálni.

A sérülékenység kapcsán eddig megfigyelt támadásfajták:

- malware telepítés
- hátsókapuk nyitása
- adatlopás
- DDoS

Az esetleges károk megelőzése érdekében a Kormányzati Eseménykezelő Központ javasolja az ***összes érintett rendszer azonnali, haladéktalan és rendszeres frissítését***, továbbá az alábbi teendők végrehajtását:

- szükségtelen bejövő forgalom blokkolása
- szükségtelen szolgáltatások letiltása
- webszerverek alacsony hozzáférési jogosultságokkal történő futtatása
- a website-okra beérkező adatok alapos, mindenre kiterjedő szűrése
- a tűzfal frissítése és folyamatos ellenőrzése
- folyamatos, akár napi többszöri rendszerfrissítés
- a sérülékenységek meglétének ellenőrzése a megadott scriptek segítségével

A sérülékenységek megléte az alább scriptek futtatásával ellenőrizhető:

A CVE-2014-6271 hivatkozási számú sérülékenység ellenőrzése:
$ env x='() { :;}; echo serulekeny' bash -c 'echo hello'

A futtatás eredménye, ha a rendszer *sérülékeny*:
$ env x='() { :;}; echo serulekeny' bash -c 'echo hello'
serulekeny
hello

A futtatás eredménye, ha a rendszer *nem sérülékeny*:

$ env x='() { :;}; echo serulekeny' bash -c 'echo hello'
bash: figyelmeztetés: x: ignoring function definition attempt
bash: hiba a függvénydefiníció betöltésekor: „x”
hello

A CVE-2014-7169 hivatkozási számú sérülékenység ellenőrzése:
$ env X='() { (a)=>\' sh -c "echo date"; cat echo

A futtatás eredménye, ha a rendszer *sérülékeny*:
$ env X='() { (a)=>\' sh -c "echo date"; cat echo
date
2014. szept. 29., hétfő, 09.21.51 CEST

Az utóbbi sérülékenységre jelenleg nem elérhető még javítócsomag.

A témában ajánlott linkek:

- http://www.cert-hungary.hu/node/275
- http://tech.cert-hungary.hu/vulnerabilities/CH-11649
- http://tech.cert-hungary.hu/vulnerabilities/CH-11663
- http://en.wikipedia.org/wiki/Shellshock_(software_bug)
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169

Kormányzati Eseménykezelő Központ
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Web: http://www.cert-hungary.hu/
Incidensbejelentés: cert@cert-hungary.hu