Shellshock-kolt? Talán igen, talán nem

PCLinuxOS Magazine – 2014. november

Írta: Paul Arnote (parnote)

2014. szeptember 24-én a bash-ban (Bourne Again Shell) biztonsági rést felfedeztek fel. A bash a PCLinuxOS alapbeállítás szerinti, szöveg alapú parancsértelmezője, ami parancssoron keresztül biztosítja a felhasználó és gépe közötti interakciót. Általában shell-ként (héj) emlegetik. A bash számos Linux disztribúcióban alapbeállítás, csakúgy mint a Mac OS X-nél.

Igen, lehet, hogy Shellshock-olt vagy. Akkor igen, ha nem tartod a rendszeredet frissen. Ám, ha rendszeresen végrehajtottad a frissítéseket (ahogy kell), akkor a rendszered már „foltozott” és immúnis ettől az leggyakoribb sérülékenységtől.

A Windows, Android és iOS felhasználókat általában ez nem érinti, legalábbis közvetlenül. Az utóbbi két rendszernél a veszély fennáll, ha a felhasználó telepített bash-t. Például az én LG2-es androidos telefonomon a Google Store-ban számos bash változat érhető el. Noha, a leírásukat olvasva nem derül ki, hogy azok a verziók érintettek-e, jobb, ha annak tételezzük fel azokat. A legtöbbjük kiadási dátuma 2014. augusztus, ami a Schellshock sérülékenység felfedezése előtti.

A bash 1989 körül jelent meg, eredetileg Brian Fox írta a GNU Project számára a Unix Bourne Shell-jének lecserélésre. POSIX kompatibilis és a csh, ksh és sh jellemzőiből is beépített dolgokat. Úgy vélik, hogy a nemrég felfedezett sérülékenység fennállt már a kezdetek óta. Mások, a sérülékenységet az 1.13-as verzióra vezetik vissza. Mindazonáltal, a bash most a 4.3.2–es verziónál jár, vagyis a sérülékenység egy ideje már létezik. Alapvetően a sérülékenység lehetővé teszi egy függvény exportálását környezeti változóként más bash példányba. Az adott függvény könnyen tartalmazhat ártalmas kódot. Tény, hogy szeptember végéig több mint 1,5 millió, a sérülékenységre alapozott próbálkozást észleltek. A próbálkozások a DDoS támadástól kezdve az irányítás és ellenőrzés átvételig terjedt.

A Schellshock sérülékenységet, hivatalos nevén CVE-2014-6271-t kitárgyaló fórumbejegyzést könnyű találni. A legjobb – és legközérthetőbb – leírást a Shellshock-ról a Wikipédiában találtam. Egy másik, hasonlóan kiváló értekezést a troyhunt.com-on láttam. A ZDNet szintén kiadott egy kitűnő GYIK-et a Shellshock-ról. Vagyis, nem mennék bele egy mélyenszántó értekezésbe a működéséről. És még csak közel sem vagyok képes arra, amire az említett kiváló források, csak úgy, mint további több ezer hasonló oldal megtett.

Mennyire komoly a Shellshock?

Ha a sérülékenységeket egytől tízig terjedő skálán kellene osztályozni, ahol az egy a legkisebb és a tíz a legnagyobb, legsúlyosabb sérülékenység, akkor a Shellshock 10-es értékű. Tény, hogy a DHS (Belbiztonsági Minisztérium) National Cyber Security

részlege és a Nemzeti Szabványügyi és Technológiai Intézet által támogatott National Vulnerability Database (Nemzeti Sérülékenységi Adatbázis) a Shellshock-ot 10-esre osztályozza.

A Shellshock idővonala

Az időpontok azért érdekesek, mert megmutatják, hogy a „szabad forrású” közösség milyen gyorsan kapcsolt a sérülékenység kijavítására. A következőkben a legfontosabbakat tartalmazó, rövidített idővonal olvasható. A teljes idővonal itt érhető el.

2014. szeptember 12: a sérülékenységről készült első jelentés.

2014. szeptember 24: a bash sérülékenységről híradás a nagyközönségnek.

2014. szeptember 24: az első, nem véglegesnek tekintett bash folt.

2014. szeptember 26: a második, szintén nem végleges bash folt.

2014. szeptember 27: megjelenik a hivatalos folt (4.3-027), ami megszünteti a Shellshock sérülékenységet.

2014. szeptember 27-e és október 5-e között további három foltot adtak ki. A legtöbb felhasználó számára a 4.3-027 rendezte le az ügyet. A többi folt a további, kiaknázható vektorokat javítja ki. Ezek a vektorok tipikusan olyan eseteket jelentenek, amik az átlag felhasználónál nem szokásosak és a 027-es folt által nem kiküszöböltek.

Ki van veszélyben?

Nos, mindenki, aki még sérülékeny (foltozatlan) bash-változatot használ bizonyos mértékig veszélyben van. Az „átlag” felhasználók kockázata minimális. De miért kockáztass, különösen amikor van javítás és elérhető? A személyes kockázatod fokozott, amikor megbízhatatlan hálózatot, pl. nyilvános wifi hozzáférési pontot használsz.

A leginkább veszélyeztetettek, akik szervert üzemeltetnek. A bash sérülékenység, rosszindulatú függvényt a környezeti változó verembe exportálva, leginkább azoknál aknázható ki, akik CGI szkripteket futtatnak másik bash példány indítására.

Ha ssh-t használsz, szintén veszélyben vagy. Ez annyit tesz, hogy egy hacker nyitott ssh portot keres és ha talál a rendszeredben, akkor a hacker a jogosultság megemelését követően könnyedén lefuttathat a rendszeredet tönkretevő rosszindulatú parancsot.

Az érintett rendszeren a jogosultság megemelése mellett a Shellshock DDoS támadásokra is használható és használták is. Vannak további, a Shellshock-hoz köthető potenciálisan veszélyes vektorok is, ezekről a korábban említett forrásokból tájékozódhatsz.

Hogyan döntsd el, hogy sérülékeny vagy-e?

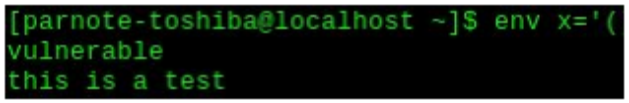
Szerencsére, annak ellenőrzése, hogy a bash verziód sérülékeny-e a szokásos expoilt-tokkal szemben elég egyszerű.

Nyiss egy terminált. A parancssorba írd be a következőt:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

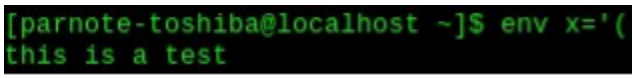
Ha a rendszered sérülékeny, akkor a következő kimenetet látod:

```
vulnerable
this is a test
```



Ha a rendszered már meg lett foltozva (pl. naprakészen tartottad a rendszert), akkor a következő kimenetet látod:

```
this is a test
```



Összegzés

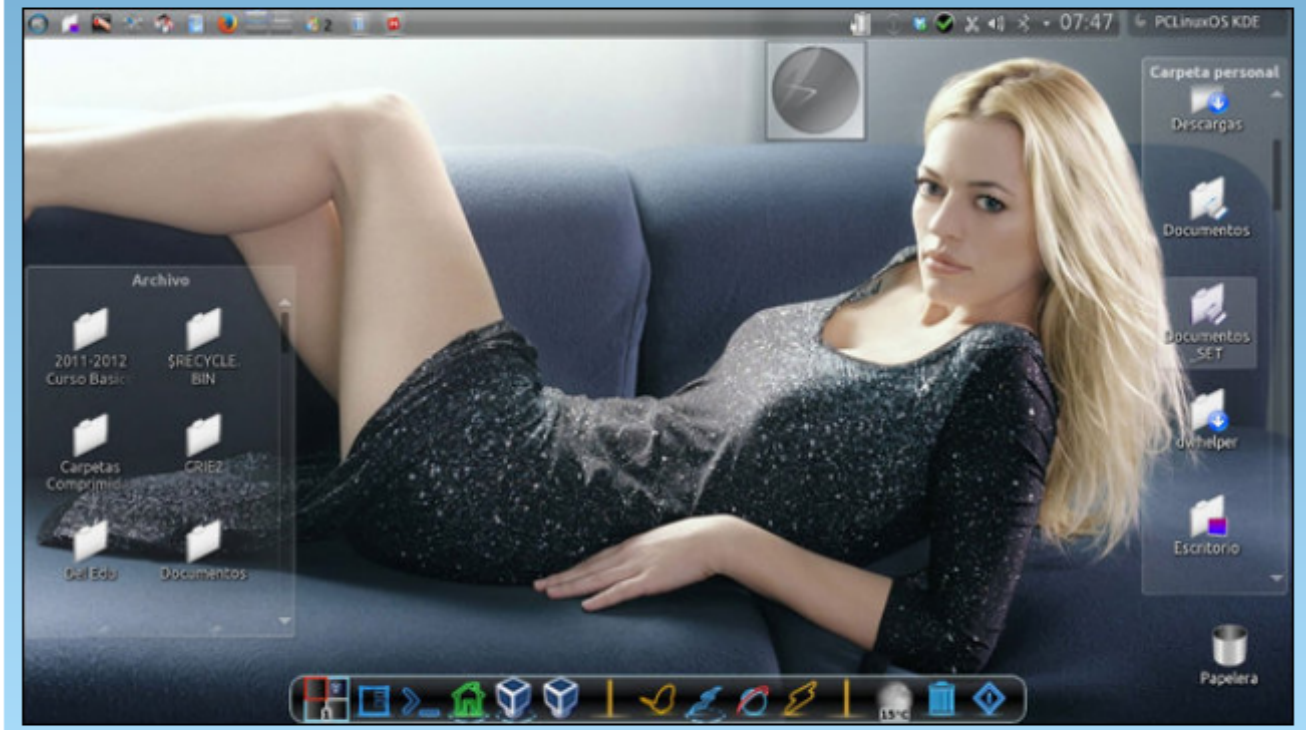
Döbbenetes, hogy a sérülékenység több mint 20 évig jelen volt és a biztonsági szakemberek sosem észlelték, vagy ismerték fel a problémát. Az sem teljesen ismert, hogy a hacker-ek mióta aknázták ki azt. Amit a biztonsági szakember most tehetnek, hogy tippelnek és reménykednek.

Egy dolog biztos: mihelyst a sérülékenység téma lett, a hacker-ek gyorsan kihasználták. Szerencsére, a két leggyakoribb sérülékenységet nagyon rövid idő alatt kiijavították. Ugyanakkor, a rendszerek sérülékenyek maradtak, amíg a frissített, foltozott bash verzió nem lett telepítve. A javítás (frissített bash) a PCLinuxOS trolóiba néhány napon belül bekerült. Ez mutatja, hogy miért fontos rendszeresen telepíteni a frissítéseket a rendszerre.

Noha a Windows-felhasználók közvetlenül nem voltak érintve (a bash a Windows-on alapból nem

fut), de mindenki, aki Internetre csatlakozik veszélyben van (volt). Tudván, hogy a hálózati szerverek jelentős része Linux-os, a személyes információik éppen annyira veszélyben voltak, mint azoké, akik bash-t alapból futtató operációs rendszert használnak. És napjainkban ritka az a számítógép, ami nem csatlakozik az Internethez.

Screenshot Showcase



Posted by Crow, on 10/17/14, running KDE.