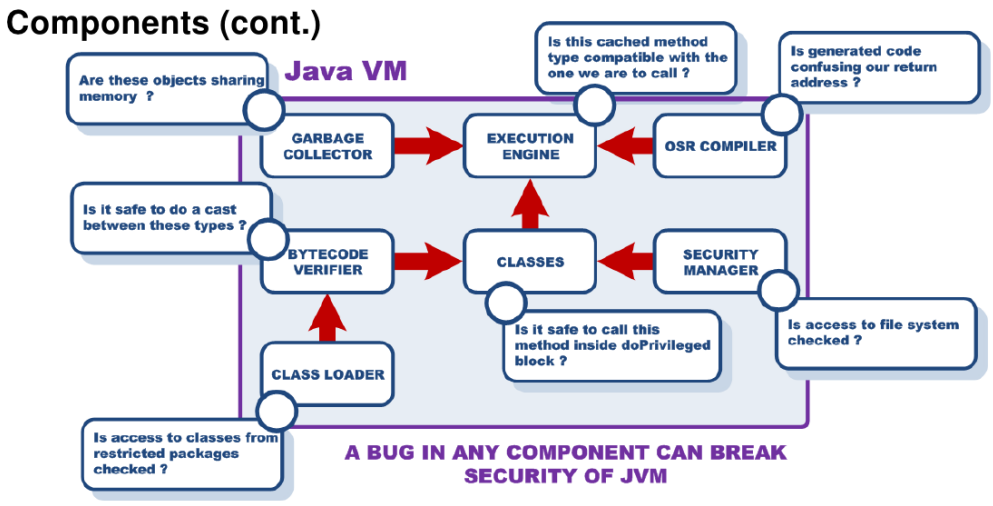
Biztonsági hibák a Java környezetben



Az idei Devoxx Java fejleszti konferencia egyik érdekes eladása Adam Gowdiak nevéhez fzdik, a bemutató vázlatát a Security vulnerabilities in Java SE linket követve olvashatjuk el, a PDF formátumú prezentációt pedig a se-2012-01-devoxx.pdf letöltésével tekinthetjük meg.

Az eladás központi témája az SE-2012-01 projekt, amely a Java futtatókörnyezet sandbox mechanizmusát veszi górcs alá, ebbl "esett ki" nyáron a hírhedt Java sebezhetség is (Java 7 sebezhetség). Úgy gondolom, hogy tapasztalt Java fejlesztknek nem okoz meglepetést, hogy a homokozóból való kitörés leginkább a Reflection API segítségével lehetséges, így az eladás nagyobb részét tekintve errl olvashatunk.

A Reflection API a Java 1.1 verzióban jelent meg, tervezésekor ügyeltek a biztonságos mködésre, de az eltelt évek alatt ez a fegyelem fellazult, így jelenleg a Java futtató környezet tele van olyan kihasználható hibákkal, amelyek súlyos problémákat tudnak okozni, mivel a sandbox környezetbl való kitörés után már nem abban az ersen szkített környezetben fut, amelyre a felhasználó gondol.

A Project SE-2012-01 egy másik megállapítása a sebezhetségek és a sandbox kitörési lehetségek száma a három nagyobb Java implementátor futtató környezetében:

VENDOR	# ISSUES REPORTED	# FULL SANDBOX BYPASS EXPLOITS
Oracle	31	17
IBM	17	10
Apple	2	1

A tanulmány utolsó negyedét a kihasználható sebezhetségek példával illusztrált listája foglalja el, illetve a cégek hibákhoz való hozzáállását – a fenti táblázatot magyarázandó:

- Oracle
  - 31 hibából 29-et javított, meglehetsen lomha tempóban
  - Akkor adott ki rendkívüli hibajavítást, amikor a proof-of-concept mellé rosszindulatú kihasználás is terjedni kezdett
  - Kritikus sebezhetség javítását ütemezte át 2013 februárra
  - A kommunikáció viszonylag részletes és rendszeres
- IBM
  - Eleinte rendkívül formális jogi szövegekkel teli válaszok
  - A 17 hibát 2 hónapos átfutással javították
- Apple
  - 5 hónapos átfutási id
  - Csendes hibajavítás (nem kommunikálták a felhasználóik felé, hogy mit és miért javítottak)
  - Eltávolították a Java környezetet a böngészkbl

Összegezve

A Java sebezhetségek okán **ajánlott a böngészben letiltani az Applet futtatás lehetségét**, és csak arra az idre engedélyezzük, amíg feltétlenül szükséges!

A tanulmány amúgy érdekes olvasmány, ajánlom minden Java fejleszt és biztonsági szakember számára... 🙂