PTA CERT HUNGARY

PUSKÁS TIVADAR KÖZALAPÍTVÁNY

Oracle Java sérülékenység összefoglaló

A PTA CERT-Hungary (Nemzeti Hálózatbiztonsági Központ) már tájékoztatást adott az Oracle Java JRE és JDK termékét érintő kritikus szoftver sérülékenységről. Jelen dokumentum egy összefoglalót tartalmaz a 2013. január 18-án, rendelkezésre álló információk alapján.

2013. január 11.

Ezen a napon jelentették a Java termékek kritikus sérülékenységét (http://tech.cert-hungary.hu/vulnerabilities/CH-8223), amelyet kihasználva a támadók tetszőleges kódot futtathatnak a sérülékeny felhasználói rendszereken. A helyzetet tovább súlyosbítja, hogy a sérülékenység kihasználását célzó exploit kód publikusan is elérhető.

Amennyiben a felhasználó megnyit egy speciálisan erre a célra készített HTML dokumentumot, a támadó tetszőleges kódot futtathat az érintett rendszeren. Az Internet Explorer web tartalmak renderelési komponense, mint a Microsoft Office vagy a Windows Desktop Search is felhasználható a sérülékenység támadási vektoraként.

2013. január 14.

Érintett verziók:
JDK és JRE 7 Update 10 és korábbiak (1.7.x / 7.x)

Nem érintett verziók:
A legfrissebb információk szerint a sérülékenység nem érinti a Java JDK és JRE 6, 5.0 és 1.4.2, valamint a Java SE Embedded JRE kiadásokat.

2013. január 15.

Az Oracle **kiadta a sérülékenység javítását célzó frissítését**. A kiadott Java 7 (Update 11) viszont **nem képes hatékony védelmet nyújtani** a felhasználókat fenyegető veszélyforrás ellen, mivel a javítás nem több, mint az alapértelmezett Java Biztonsági Szint (Java Security Level) Közepesről Magasra állítása. Ezzel a probléma nem kerül megoldásra, csak egy esetleges incidens felelősségét áthárítja a felhasználóra, mivel a Java ezzel a beállítással minden esetben figyelmezteti a felhasználót, ha egy aláíratlan Java applet-et vagy Java Web Start alkalmazást akar futtatni és felhasználó döntésére bízza annak végrehajtását.

A **sérülékenység nem érinti a szervereken futó Java verziókat**, a standalone desktop vagy a beágyazott Java alkalmazásokat.

Az Egyesült Államok Belbiztonsági Minisztériuma megismételte azt a figyelmeztetését, hogy a **Java sérülékenység továbbra is biztonsági veszélyeket hordoz magában** azután is, hogy az Oracle kiadta a nemrég felfedezett 0-day sérülékenység miatt készített legfrissebb verziót.

Amennyiben a támadó sikeresen kódot tud futtatni a felhasználó rendszerén, akkor képes lehet személyes információkat szerezni, azonosítókat lopni, vagy botnet hálózatba léptetni a fertőzött gépet.

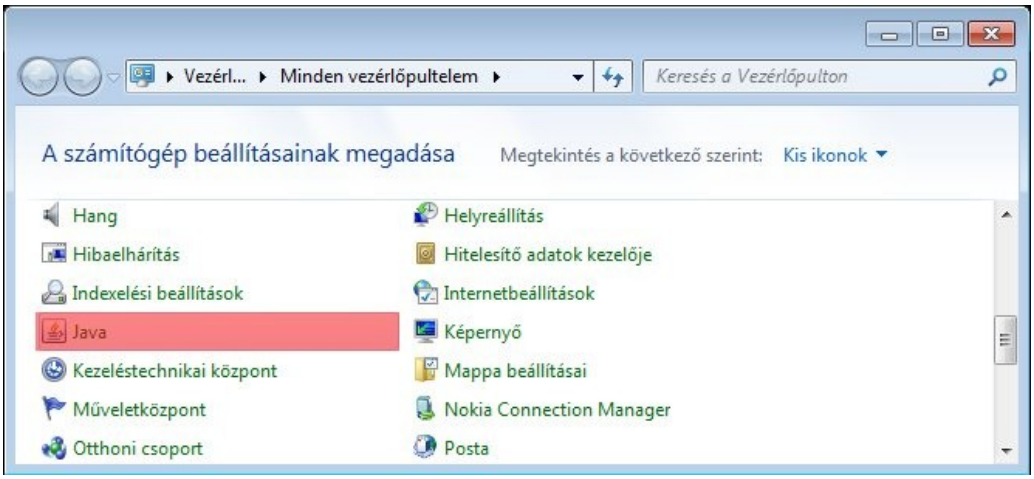
Budapest VI., Munkácsy M. utca 22.
Levélcím: 1398 Budapest Pf. 570 Tel.: 301-2080 Fax: 353-1937 E-mail: info@cert-hungary.hu

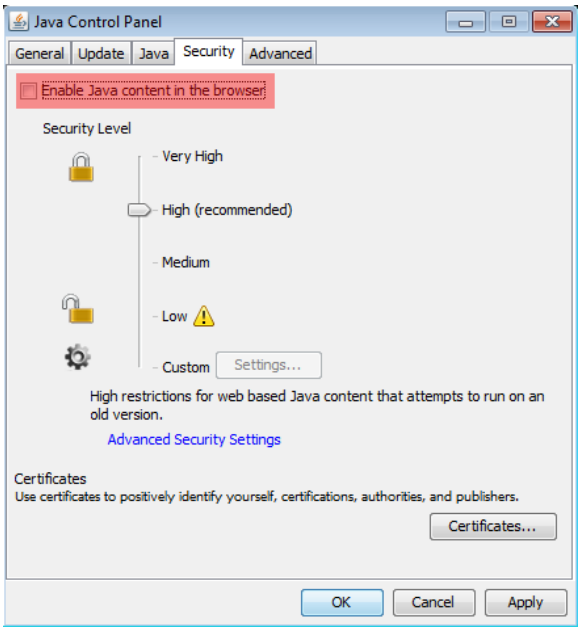
Javaslat

Központunk továbbra is javasolja a **Java tartalmak kikapcsolását a böngészőkben**, illetve amennyiben a kliensen nincs szükség a Java-ra, úgy javasolt annak kliensen történő tiltása/kikapcsolása is. A Java 7 update 10-től kezdődően lehetőség van a Java tartalmak kikapcsolására a böngészőkben. Az olyan rendszerek esetén ahol magasabb biztonsági szintre van szükség, lehetőség van a Java alkalmazások (aláírt és aláíratlan) böngészőben történő futásának teljes megakadályozására. Ehhez a Java Vezérlőpulton a Biztonság fülön a „Java tartalom engedélyezése a böngészőkben" lehetőséget ki kell kapcsolni.

Bővebb információ a Java tartalmak kikapcsolásáról (angol):
http://www.kb.cert.org/vuls/id/636312#solution

Java tartalmak kikapcsolása a böngészőkben Windows 7 és Windows XP esetén
A Start menü, Vezérlőpultban a Java ikonra kattintva a következő beállítást kell elvégezni:





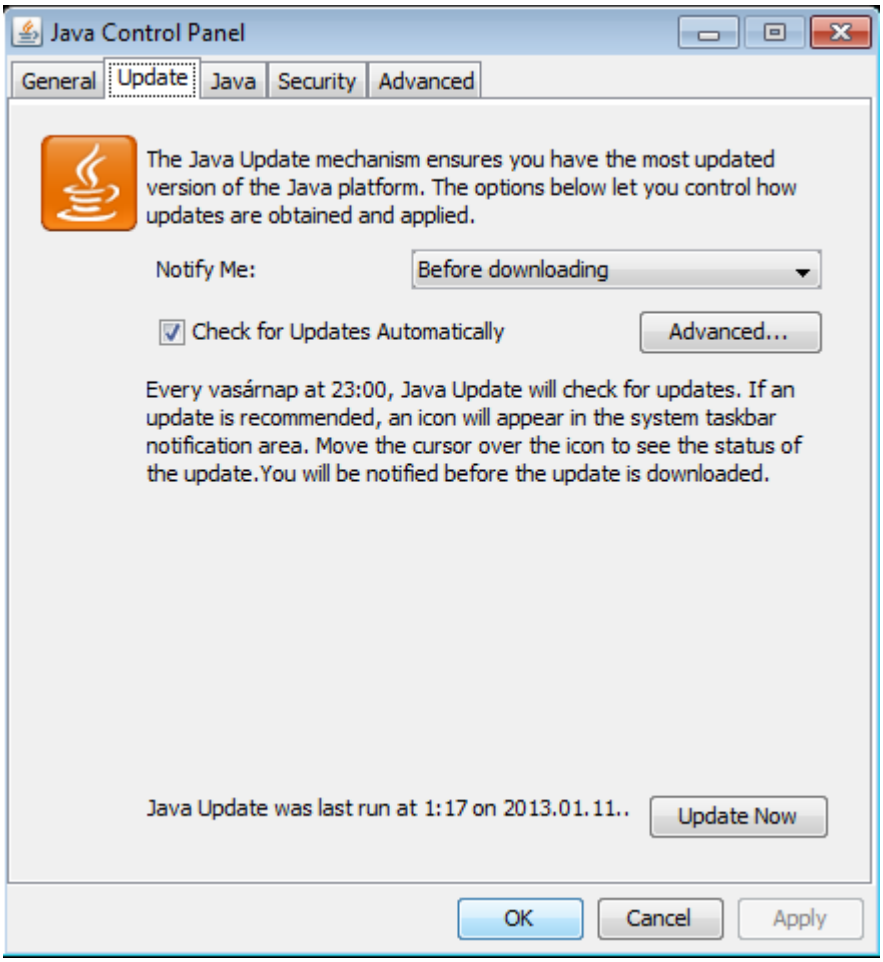
Budapest VI., Munkácsy M. utca 22.
Levélcím: 1398 Budapest Pf. 570 Tel.: 301-2080 Fax: 353-1937 E-mail: info@cert-hungary.hu

Java frissítése

A frissítés letölthető az Oracle hivatalos weboldalán keresztül a következő elérhetőségeken:

- http://www.java.com/en/download/manual.jsp (JRE)
- http://www.oracle.com/technetwork/java/javase/downloads/index.html (JDK)

A Start menü, Vezérlőpultban a Java ikonra kattintva is elvégezhető a frissítés az „Update Now” gombra kattintva:



A sérülékenységről szóló részletes leírás

http://tech.cert-hungary.hu/vulnerabilities/CH-8223

Budapest VI., Munkácsy M. utca 22.
Levélcím: 1398 Budapest Pf. 570 Tel.: 301-2080 Fax: 353-1937 E-mail: info@cert-hungary.hu