Mitos y realidades de la seguridad en Java

Víctor Orozco

Nabenik

11 de octubre de 2014

#JavaDayGT2014

Disertativa sin código

FayerWayer

ESTAS LEYENDO

El Departamento de Seguridad Nacional de EE.UU. recomienda dejar de utilizar Java

RAFA GARCÍA

CES 2013: Babe Report 3: TFF

hace 2 años 227

JUAN PABLO OYANEDEL

Estados Unidos ya implementa software para la predicción de crímines

hace 2 años 460

PABLO GUTIERREZ

CES 2013: Paramount lanza aplicación interactiva para el estreno de "Star Trek Into Darkness"

hace 2 años 258

JUAN PABLO OYANEDEL

Pese a Windows 8, despachos de PCs fueron menores a lo esperado a finales del 2012

hace 2 años 229

1.274 12.123

El Departamento de Seguridad Nacional de EE.UU. recomienda dejar de utilizar Java

JUAN PABLO OYANEDEL 11 ENERO 2013 SOFTWARE

Esto, a raíz de la vulnerabilidad que salió a la luz el día de ayer. Además, Apple desactivó automáticamente Java en OS X y se revelaron nuevos usos que los piratas están aprovechando para este agujero.

Ayer 10 de enero de 2013, salió a la luz una grave vulnerabilidad que afecta al software Oracle Java para las plataformas Windows, OS X y basadas en Linux, la que permite a un pirata informático ejecutar cualquier código en la computadora de la víctima, quien debe además entrar a un sitio con HTML malicioso para ser afectado. A raíz de esto, casi todas las empresas de seguridad dijeron al unísono que debíamos dejar de utilizar Java en nuestros sistemas.

por JUAN PABLO OYANEDEL
3767 posts

TODO SOBRE

Linux
Linux, a veces nombrad...

VER MÁS

BHEK

BLACKHOLE EXPLOIT KIT

CEK

economy

Java Security Flaw Is Repaired; Experts Still Recommend Disabling It

by BILL CHAPPELL
January 14, 2013 2:45 PM ET

Days after the Department of Homeland Security said computer users should remove the latest versions of its Java software, Oracle Corp. says it has fixed the flaw, in a new update released Monday. As we reported Friday, hacking groups included the Java 7 vulnerability in new "exploit kits" this year.

Oracle provides instructions for updating to Java 7, update 11 on its website, saying the update raises the default security level for Java applets from Medium to High — which means that "the user is always warned before any unsigned application is run to prevent silent exploitation," the company says in its release notes.

But the experts who highlighted the Java 7 flaw say that even though it's fixed, users should beware, as other security problems could arise in the software.

"Unless it is absolutely necessary to run Java in web browsers, disable it... even after updating," recommends Carnegie Mellon University's CERT computer security site.

News of the Java 7 flaw, which can allow hackers to take over a computer, worried many of the millions of people whose computers use the software. It also set off confusion, and calls for Oracle to "rewrite Java from scratch," as PC World reports.

Less than a week after fix, Java is broken yet again

By Christopher White · Jan 20, 2013 · HOT! 33

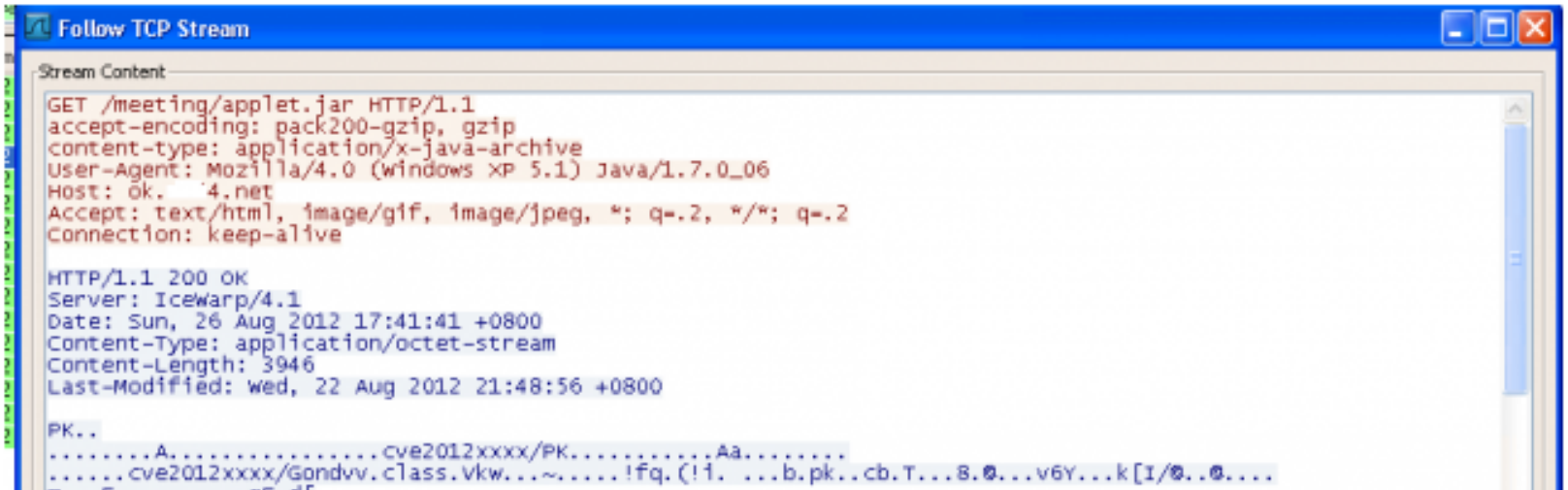
With over a billion installations, Java is in everything from your computer to your thermostat, and nefarious hackers are taking note. Attacks have been coming fast and furious, with Flashback hitting the Mac platform last spring, and more recent updates impacting all platforms. The United States government even recommended that users disable Java from their browsers.

Now it appears there is yet another Java vulnerability running rampant in the world, despite the fact that it was updated again last week. According to PC World, researchers at Poland-based Security Explorations found not one, but two new vulnerabilities that allow attackers to run arbitrary code on

Critical flaw under active attack prompts calls to disable Java

Oracle's Java framework is once again under attack, thanks to new vulnerability.

by **Dan Goodin** - Aug 27 2012, 10:44am CST



¿Porqué fue importante?

From laptops to datacenters, game consoles to scientific supercomputers, cell phones to the Internet, Java is everywhere!

- 97% of Enterprise Desktops Run Java
- 89% of Desktops (or Computers) in the U.S. Run Java
- 9 Million Java Developers Worldwide
- #1 Choice for Developers
- #1 Development Platform
- 3 Billion Mobile Phones Run Java
- 100% of Blu-ray Disc Players Ship with Java
- 5 Billion Java Cards in Use
- 125 million TV devices run Java
- 5 of the Top 5 Original Equipment Manufacturers Ship Java ME

RISK

9/26/2012
10:39 AM

Mathew J. Schwartz
News

Connect Directly

0

Java Vulnerability Affects 1 Billion Plug-ins

Another week, another Java vulnerability--only this one affects all versions of Java released in the past eight years.

Anyone still using a Java plug-in in their Web browser, beware: Another major, new--and as yet unpatched--vulnerability has been spotted in Java.

Unfortunately, unlike a number of the other, recently spotted Java bugs, the latest security issue affects not just the current, version 7 of Java, but also versions 5 and 6. In other words, every version of Java released for the past eight years, collectively used by approximately one billion people, is vulnerable to the exploit.

Aumento de la superficie de ataque.
Write (a exploit) once, run (it) everywhere.

Javas

- Java Card
- Java ME (BD-J, dumbphones)
- Java SE (Escritorio, Applets)
- Java EE (Web, SOA, personas con corbata)

¿Y que pasó desde entonces?

Acciones

- Nuevo modelo de lanzamientos
  - Limited updates (actualizaciones) - múltiplos de 20
  - Critical patch updates - Impares en multiplos de 5
  - **8u20** 8u25 8u31 8u35 **8u40** 8u45 **8u50**
- Nuevo jefe de seguridad - http://www.securitycurmudgeon.com/2014/04/spotlight-on-java-se-8-security.html
- Grupo de seguridad en OpenJDK - http://openjdk.java.net/groups/security/
- Nuevo security track a partir de JavaOne 2013

http://java-0day.com/ 11-10-2014

Days since last known Java 0-day exploit

Previous high score: 87

General info

Java-related CVEs:
web.nvd.nist.gov

No glove, no love:
How to be safe?

```
navigator.javaEnabled() == true
```

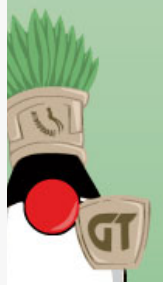
Latest patch:
Java 7u51

Latest 0-day(s) info

Is it still a threat? istherejava0day.com
a.k.a. "is the latest patch useless yet?"

Fulldisclosure
http://seclists.org/fulldisclosure/2013/Jul/172
(SE-2012-01 issue #69)

Fulldisclosure
http://seclists.org/fulldisclosure/2013/Apr/194
(SE-2012-01 issue #61)



¿Como debo protegerme?


Confidentiality
Integrity
Data &
Services
Availability

-1. Evitar pentesting king/kids

PENTEST KING

6 GREAT MODELS TO CHOOSE FROM! A TEST FOR ANY BUDGET!

If you're in the market for a new penetration test, look no further!

Level 1 – THE CLASSIC

This classic is sure to pretend to do something!

CALL FOR A QUOTE!

Level 2 – SMASH AND GRAB!

Get ready to have your network DESTROYED!!!!

Features:

- No regard for your business!
- Huge reports
- Scanners, scanners, scanners!

CALL FOR A QUOTE!

Level 3 – THE PACIFIER

You'll get a great report every time (that doesn't mean everything is ok...)

Features:

- Might sell or service your office printer!
- Wont break anything!

CALL FOR A QUOTE!

Level 4 – THE RFCist

The tester knows EVERYTHING! Except the why part!

Features:

- Technical genius
- Anti-social

CALL FOR A QUOTE!

Your score: **100!**

Level 5 – THE AUDITOR

After careful risk analysis, your score is.....!

Features:

- Tight, neat packages
- No technical know-how
- Lots of letters after their names

CALL FOR A QUOTE!

Level 6 – THE RICH KID

They spent all their money on this tool... It's got to work!

Features:

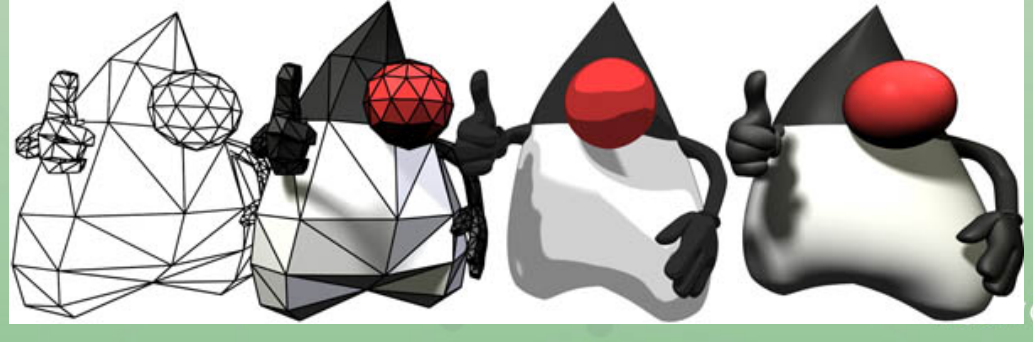
- Loves buzzwords!
- Includes really expensive accessories

CALL FOR A QUOTE!

0. Conociendo NUESTRO java

Javas

- **HotSpot** (Oracle)
- JRockit (Oracle)
- OpenJDK (Oracle)
- Jikes (Eclipse)
- HP-UX Java (HP)
- J9 (IBM)
- Zing (Azul Systems)
- Zulu (Azul Systems+OpenJDK)



1. (Intentar)Ir a la velocidad de los atacantes

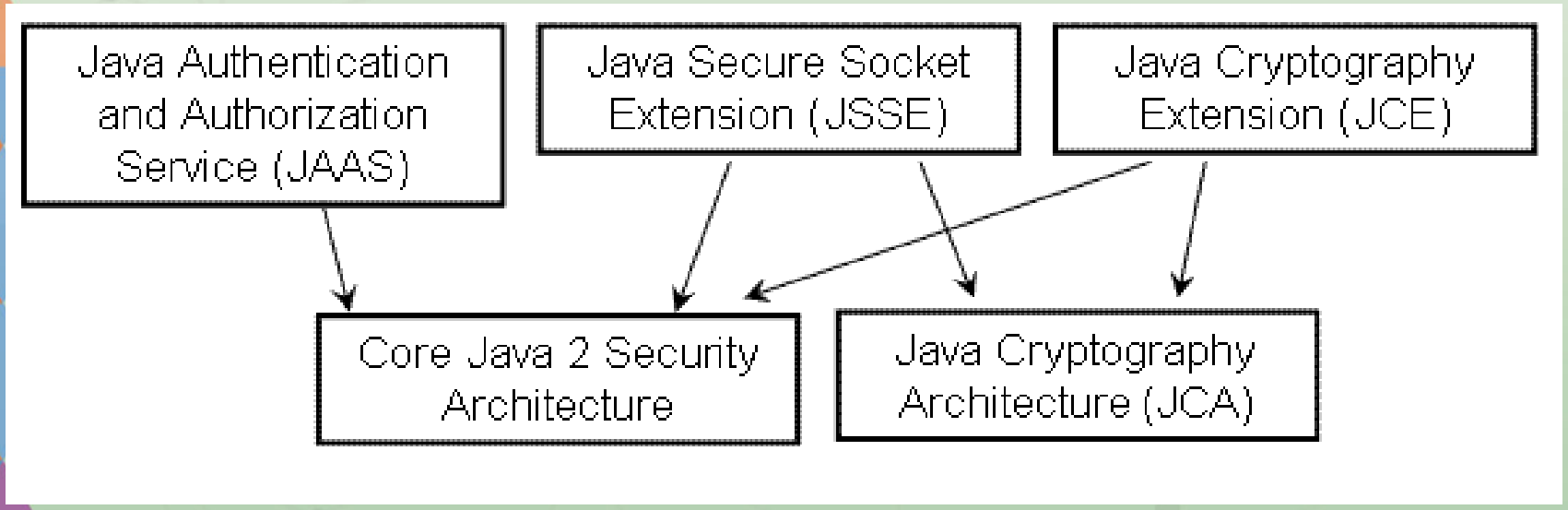
Recursos

- CVE - `http://web.nvd.nist.gov/view/vuln/search-results?query=java&search_type=all&cves=on`
- Oracle Software Security Assurance - `https://blogs.oracle.com/security/`
- Debian Advisories - `https://www.debian.org/security/`
- RedHat Advisories - `https://access.redhat.com/security/updates/advisory`

2. Conociendo los modelos de seguridad de Java

Autenticación y autorización

Modelo JavaSE



Modelo JavaEE

- Declarativa
  - Basado en el contenedor
  - Modelo de autenticación - Credenciales, OpenID
  - Modelo de autorización - Basado en roles
- Programática
  - EJBContext
  - HttpServletRequest

3. Programando de forma segura

Buenas practicas de programación

- Seguridad = Requerimiento funcional
- Identificación y corrección de riesgos
- Patrones de seguridad (reducción de superficie de ataque, privilegios mínimos, defensa en profundidad)
- Documentación de auditorias

4. Desplegando de forma segura

Despliegues seguros

- Maven central - `http://www.infoq.com/news/2014/08/Maven-SSL-Default`
- Server JRE - `http://www.oracle.com/technetwork/java/javase/7u21-relnotes-1932873.html#serverjre`

5. Utilizando soluciones ya probadas

OWASP Java Enterprise Security API

Tipo: Biblioteca
Modo de uso: Programático
Características principales: Criptografía, filtros, reglas de validación, tags JSP, rutinas seguridad

OWASP Java Encoder

Tipo: Biblioteca
Modo de uso: Programático
Características principales:
XSS

Bouncy Castle

Tipo: Biblioteca
Modo de uso: Programático
Características principales:
API Ligera (funciona con JME)
Proveedor para Java Cryptography Extension
Generador y procesador de certificados (S/MIME, OCSP, TSP, CMP, OPENPGP) Jar firmado y compatible con Hotspot

Jasypt

jasypt.
JAVA SIMPLIFIED ENCRYPTION

Tipo: Biblioteca
Modo de uso: Programático
Características principales:
API Ligera (funciona con JME), Estándares avanzados de seguridad, Integración automática con Hibernate, Spring y Spring Security, Cifrado de alto rendimiento, A diferencia de bouncy castle, Jasypt se enfoca solo en java

Spring Security

Tipo: Biblioteca
Modo de uso:
Programático+Declarativo
Características principales:
Integración automática con spring, Soporte para inyección de dependencias, Acoplamiento debil, los componentes son facilmente reemplazables, Expression language (reglas), Autorización de peticiones HTTP, Autenticación externa (LDAP, JDBC, Kerberos, AD), Encripción de passwords, Tag

Apache Shiro

Tipo: Framework
Modo de uso:
Programático+Declarativo
Características principales:
Autenticación y autorización basada en roles, Criptografía, Administración de sesiones, Autenticación externa (LDAP, JDBC, Kerberos, AD) y soporte para Single Sign On, Pocas dependencias, Acoplamiento debil, componentes fácilmente reemplazables.

Gracias

- E-mail: tuxtor@shekalug.org
- Blog: http://tuxtor.shekalug.org
- Twitter: @tuxtor
- Fuentes: http://github.com/tuxtor/slides