



Vulnerability Notification

Version 1.0 – 11.01.2013 (Final)

Notification (VN2013011101)

Classification : PUBLIC / TLP WHITE

Department : GOVCERT.LU



Revision control

Version	Index	Date	Modification description	Origin of the modification request (name, surname and function)
1	0	11.01.2013	Final version (creation)	GOVCERT.LU



Objet

Vulnérabilités dans Oracle Java

Classification

TLP-WHITE

<http://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf>

Destinataires

GOVCERT.LU Constituency (contacts techniques)

Criticité

Haute

Impact

Exécution de code à distance

Systèmes concernés

Tout plugin navigateur Oracle Java 7 jusqu'à update 10

Oracle Java 6 pas encore confirmé, EOL Féb 2013

A noter que pour Java 6 d'autres vulnérabilités non corrigées existent.

Actuellement seulement une partie des logiciels antivirus détectent les exploits relatifs à cette faille.

A ce jour, de nombreux malwares utilisent activement cette vulnérabilité pour compromettre les systèmes cibles.

Correctif

A ce jour aucun correctif n'a été mis à disposition par Oracle.

Mitigation

Limiter l'utilisation d'Internet Explorer au stricte minimum et préférer les navigateurs Firefox ou Chrome. Lorsque vous utilisez Chrome ou Firefox, activez l'option click-to-play pour éviter le lacement automatique de contenu java non désiré. A noter que cette option affecte tous les sites qui utilisent du contenu active comme du Java, Flash etc..



Pour plus d'informations sur l'activation de l'option click-to-play, veuillez consulter la documentation fournie par CASES.

https://www.cases.lu/vulnerabilite_extremement_critique_dans_java.html

Références

- <http://stopmalvertising.com/malware-reports/analysis-of-cve-2013-0422-a-new-0-day-java-exploit.html>
- <http://labs.alienvault.com/labs/index.php/2013/new-year-new-java-zero-day/>
- <http://malware.dontneedcoffee.com/2013/01/0-day-17u10-spotted-in-while-disable.html>
- https://www.cases.lu/vulnerabilite_extremement_critique_dans_java.html