

# Failles critiques dans Java

Alors que Sun Microsystems publie le code source de Solaris (lire notre article), le constructeur doit faire face à deux failles qualifiées de »

*critiques* » affectant son produit vedette, Java. Corrigées, les updates sont disponibles sur son site. La première vulnérabilité impacte **Java 2 Platform Standard Edition**. Elle pourrait être exploitée par un attaquant distant afin de compromettre un système vulnérable. Selon le site de veille FrSIRT, le problème résulte d'une erreur inconnue présente au niveau de la gestion de certaines 'applets' malformées. La faille peut être exploitée via une page Web malicieuse afin de lire/placer des fichiers arbitraires sur un système vulnérable ou exécuter des application locales avec les privilèges de l'utilisateur connecté. Les versions impactées sont J2SE 1.4.2\_07 et inférieures (Windows, Solaris et Linux), Java 2 Platform Standard Edition(J2SE) 5.0 (Windows, Solaris et Linux) et Java 2 Platform Standard Edition(J2SE) 5.0 Update 1 (Windows, Solaris et Linux). La solution consiste à migrer vers Java 2 Platform Standard Edition(J2SE) 5.0 Update 2 et J2SE version 1.4.2\_08. **La seconde faille critique** touche **Java Web Start**. Mêmes conséquences: elle pourrait être exploitée par un attaquant distant afin de compromettre un système vulnérable. Toujours selon FrSIRT, le problème résulte d'une erreur dans les modules exécutables « javaws.exe » (Windows) et « javaws » (Solaris and Linux) qui ne manipulent pas correctement certains fichiers « JNLP » spécialement conçus. La vulnérabilité pourrait être exploitée via une page Web, afin d'installer des fichiers malicieux sur un système vulnérable (virus, 'trojan'...). Les versions impactées sont Java Web Start dans Java 2 Platform Standard Edition (J2SE) 5.0 (Windows, Solaris et Linux) Java Web Start dans Java 2 Platform Standard Edition (J2SE) 5.0 Update 1 (Windows, Solaris et Linux). La solution consiste à utiliser Java Web Start in Java 2 Platform Standard Edition (J2SE) 5.0 Update 2. FrSIRT précise également que les navigateurs Internet Explorer, Mozilla, Firefox et Opera peuvent être affectés par cette vulnérabilité s'ils utilisent une version vulnérable de Java.