

Critical Flaws Found in Java Development Kit

May 18 2007

The two flaws could be exploited remotely by hackers, with one resulting in the possible execution of code.

Two vulnerabilities open to remote exploitation by hackers have been found in Java Development Kit, one of which could be used to take over a compromised system.

JDK (Java Development Kit) is a software development tool made by Sun Microsystems specifically for Java users. The vulnerabilities were rated "critical" by FrSIRT (French Security Incident Response Team), a security research organization based in France.

One flaw is caused by an integer overflow error in the image parser when processing ICC profiles embedded within JPEG images, according to FrSIRT researchers.

Security experts at Secunia outlined the dangers of the flaw in a separate advisory. "This can be exploited to crash the JVM and potentially allow the execution of arbitrary code by e.g. tricking an application using the JDK to process a malicious image file," Secunia security experts stated.

The second vulnerability is caused by an error in the BMP image parser when processing malformed files on Unix/Linux systems, which could be exploited by attackers to cause a denial of service. Both flaws affect Sun JDK version 1.x.

Users can find an answer to both vulnerabilities by upgrading to [JDK versions](#) 1.5.0_11-b03 or 1.6.0_01-b06.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: Critical Flaws Found in Java Development Kit (2007, May 18) retrieved 23 April 2024 from <https://phys.org/news/2007-05-critical-flaws-java-kit.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.