

J2ME security vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0937.html>

From: Adam Gowdiak (zupa_at_man.poznan.pl)

Date: 10/22/04

Date: Fri, 22 Oct 2004 14:01:10 +0200

To: full-disclosure@lists.netsys.com, bugtraq@securityfocus.com

Hello all,

Since I received information from SUN Microsystems that they did not plan to release Sun Alert for the issues I found in their CLDC [1] reference implementation, I would like to announce the following.

I found two very serious security vulnerabilities in Java technology for mobile devices (Java 2 Micro Edition) that might be affecting about 250 millions [2] of mobile phones coming from Nokia, Siemens, Panasonic, Samsung, Motorola and others [3]. Information about these flaws has been published at Hack In the Box Security Conference [4] earlier this month in Kuala Lumpur, Malaysia.

Both vulnerabilities are implementation flaws in bytecode verifier component of KVM (Java Virtual Machine for mobile devices) developed by SUN Microsystems. Each of the flaws can be used to completely break Java security (Java type and memory safety) on a mobile device and to obtain access to the phone data and underlying operating system's functionality.

I verified on my Nokia DCT4 phone that malicious code exploiting one of the flaws can steal data from the phone (i.e. phonebook, SMS messages), establish communication with the Internet, send arbitrary SMS messages, write permanent memory of the phone (FLASH), interfere with or intercept IPC communication occurring between native Nokia

Full-Disclosure: J2ME security vulnerabilities

OS tasks, install resident code on the phone. Any of the aforementioned actions can be conducted without user knowledge and permission.

I would like to emphasize that although escaping the KVM sandbox and breaking Java type and memory safety is almost straightforward, conducting malicious actions on a given device is rather difficult as it usually requires deep knowledge about the internal operation of the underlying OS (I spent four months reverse engineering Nokia OS before I could do anything malicious from Java application on my phone).

I plan to release a research paper with all the details about the flaws including device specific information and some additional material that didn't fit into my HITB talk, in a couple of months (1Q 2005).

Best Regards
Adam Gowdiak

Security Team of
POZNAN SUPERCOMPUTING AND NETWORKING CENTER
<http://www.man.poznan.pl>

[1] <http://java.sun.com/products/cldc/>

[2] http://media.corporate-ir.net/media_files/NYS/NOK/Beijing/mestaranta.pdf

[3] <http://jal.sun.com/webapps/device/device>

[4] <http://conference.hackinthebox.org>