

[NEWS] Jetty Session ID Prediction Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00016.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2007 10:57:14 +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>

Jetty Session ID Prediction Vulnerability

SUMMARY

Different versions of Jetty, the popular java web server, are vulnerable to a session id prediction attack.

DETAILS

Vulnerable Systems:

* Jetty versions prior to 4.2.27, 5.1.12, 6.0.2 and 6.1.0pre3

Immune Systems:

* Jetty versions 4.2.27, 5.1.12, 6.0.2 and 6.1.0pre3.

Jetty uses `java.util.Random` to generate session ids. The internal state of this generator can be easily discovered, leading to an attacker being able to hijack existing and future sessions.

`java.util.random` implements a linear congruential generator, of the following form:

```
synchronized protected int next(int bits) {  
    seed = (seed * 0x5DEECE66DL + 0xBL) & ((1L << 48) - 1);  
    return (int)(seed >>> (48 - bits));  
}
```

}

Jetty generates a 64-bit session id by generating two 32-bit numbers in this way, so we end up with an encoded 64-bit integer. By decoding the integer and splitting it into its two component 32-bit integers, we can easily brute-force the generator's internal state. Once the state is discovered, the generator can be run both forwards and backwards, so an attacker can determine previously generated session ids, as well as session ids that have not yet been generated. This allows the attacker to hijack any existing session, and perform any actions that the original user of the session could perform. Obviously the severity of this issue varies from application to application but we believe it warrants at least a "high" risk rating.

NGS have developed proof of concept code for this issue that implements a session predictor for this bug. It takes a session id as input and outputs candidates for the next 5 and previous 5 session ids. It is necessary to output 7 candidate session ids for each iteration because Jetty encodes the session id in a number base from 30 to 36 depending on the millisecond in which the session id was generated. The underlying 64-bit integer is the same, just represented in bases 30-36.

Here is some example output:

```
H:\jetty_rand\Debug>jetty_rand.exe g4sse9e7fs5ee
```

```
Radix: 30
```

```
Found seed: 5346772124980067
```

Session -5:

```
27s4jsk03074k  
1gbb661e0l6mp  
11ctqbu24shqo  
nqqa46cv6ovh  
h4xlr7d8n98c  
cg9x29g6vfna  
9568uhp0c7yw
```

Session -4:

```
586o97hbtkkis  
3h9o0c9eglm5q  
2dpgen12bekgo  
1mf3ar81r4e7d  
15vq2mdv83nmo  
t13aedmjm4ts  
lamwq2jurlzs
```

Session -3:

```
c2kqln033ior  
8d98tft18mgj  
5u715san1m0b  
47rifnwhompl  
31pb1t2496ef
```

[NEWS] Jetty Session ID Prediction Vulnerability

27mbqm91n0gc
1mksf8xjn6kr

Session -2:
h5n7ft13ak1nr
biif83e4tlq37
7tj3f6tclak5h
5fpk27ulvu2nu
3s5vpubx7ekc9
2om684eem9iy2
1xf0lar1nqpwx

Session -1:
66isdajhm658g
46317trqe65oo
2rod18h2bjkb4
1wdl0j3wqr6tj
1d3hc9k0gm9ja
y8hj85q65rxq
p49erbpgioo4

Session 0:
g4sse9e7fs5ee
as3iai qcjo82g
7eeb56egthkrm
54w87w5wtpwfk
3kdimj6vemoce
2iybbcycjqk9
1t9qijf82uk52

The issue affects a great many products that are based on Jetty, such as Apache Geronimo:

<<http://geronimo.apache.org/>> <http://geronimo.apache.org/>

The latest version (2.0) of Geronimo is not vulnerable to this issue. Version 1.1 and prior are vulnerable however, and this issue can be used to hijack a session to the administrative console.

A further 98 projects based on Jetty are listed on the Jetty website at:
<<http://www.mortbay.com/powered.html>> <http://www.mortbay.com/powered.html>

Fix:

This issue was fixed in the source code on the 22nd of November 2006, less than 6 hours after it was reported. The issue is fixed in released versions 4.2.27, 5.1.12, 6.0.2 and 6.1.0pre3.

The changes can be viewed here:

<<http://fisheye.codehaus.org/changelog/jetty/?cs=1274>>
<http://fisheye.codehaus.org/changelog/jetty/?cs=1274>

[NEWS] Jetty Session ID Prediction Vulnerability

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@xxxxxxxxxxxxxxxx>>
NGSSoftware Insight Security Research.

=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.