

[NT] WebSphere Cookie and Session-id Predictability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0008.html>

From: support@securiteam.com

Date: 10/03/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] WebSphere Cookie and Session-id Predictability

Message-Id: <20011003212751.2EB3A138C2@mail.der-keiler.de>

Date: Wed, 3 Oct 2001 23:27:51 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

WebSphere Cookie and Session-id Predictability

SUMMARY

IBM WebSphere can generate session-ids that are put into cookies for users, to be able to supply user tracking, e.g. user authenticates with user-id and password, and access to data is checked by checking if the session-id is authenticated or not. A security vulnerability in the product allows attackers to analyze the generated cookies, and to easily predict what the next one will look like. This may enable them to bypass the cookie-based authentication.

DETAILS

Vulnerable systems:

WebSphere version 4.0

Example:

SessionID TIME

TWGYLZIAAACVDQ3UUSZQV2I 10:27:12

TWGY0WYAAACVFQ3UUSZQV2I 10:27:13

TWGNZAAAACVHQ3UUSZQV2I 10:27:14

Securiteam: [NT] WebSphere Cookie and Session-id Predictability

```
TWG0BUYAAACVJQ3UUSZQV2I 10:27:15
TWG0VIAAAACVLQ3UUSZQV2I 10:27:16
TWG1ICIAAACVNQ3UUSZQV2I 10:27:17
TWG111YAAACVPQ3UUSZQV2I 10:27:18
xxxx y
```

You can see that for seven requests, only five characters changed, and:

- * The characters A–Z and 0–9 are used, hence 36 combinations possible per char
- * The session-id is based on two counters that are counted up, the rest of the string seems to be fixed.
- * The first counter (xxxx) seems to count milliseconds (TWGxxxx), but counts a bit too slow (see seconds 15 and 16, where both first rows of the counters start with a 0). This is actually a counter that increases 65536 times per second and is then encoded to the A–Z0–9 format.
- * If you collect many session-ids, you will see that the most significant char of the first counter are 95% of the time showing a Y, I, A or Q. The reason for that is (my guess) that the clock of the machine only can increase 7.500–10.000 times instead of 65536 because it is not a real-time clock and the server type is not a crazy.
- * The second counter (y) is increasing by two every second.

Impact:

If an attacker knows the time of the server he connects to (even with SSL encrypted), he attacker can issue requests with changing session-ids until it is the correct one. If an attacker just wants to have any user data, he can constantly try some guessing.

As the first counter only has 7.500–10.000 values per second, and the seconds counters just increases approx. once per second (or perhaps per request), the session-id can have 7.750 to 10.500 different values. If a user is normally connected for 15 minutes after authentication to an eCommerce system (and does not forget to logout, otherwise the time is extended by the session timeout). As an attacker is likely to succeed after 50% of the key space, he needs 3.875 to 5.250 attempts, so 4 to 5 requests per second are enough.

Solution:

http://www6.software.ibm.com/dl/websphere8/wscorsvc-i?S_PKG=dl3_023ww => PQ47663V302 – This fix replaces PQ46762. Session id generation is more random; Fixes null pointer exceptions in invalidation path; Fixes DB2 out of handles exceptions in invalidation path; Makes authorization association with session configurable using system property; Fixes creation of multiple session contexts for same web applications under stress start.

ADDITIONAL INFORMATION

The information has been provided by <mailto:marc@suse.de> Marc Heuse.

=====

Securiteam: [NT] WebSphere Cookie and Session-id Predictability

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.

-
- **Previous message:** support@securiteam.com: "[\[UNIX\] Multi-Vendor Format String Vulnerability in ToolTalk Service](#)"
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)