

[NT] Session Token Remains Valid After Logout in IBM Lotus Domino Web Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00016.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 13 Sep 2006 10:36:09 +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>

Session Token Remains Valid After Logout in IBM Lotus Domino Web Access

SUMMARY

In Lotus Domino Web Access (DWA) 7.0.1, the session token used to identify the user (called "LtpaToken") is not invalidated on the server upon user logout. The cookie is removed from the browser, but the token continues to be recognized by the server until a configurable expiration time is reached.

DETAILS

Attack Overview:

The most likely attack scenario is session hijacking or session stealing. Knowing a valid session token would allow a malicious person to access all functionality of the web application (except changing password, which requires knowledge of the current password). Lotus DWA is a personal information management application that includes e-mail, calendar, and task management. By hijacking (or stealing) a session, an attacker is able to impersonate a legitimate user, and can read the user's e-mail, send e-mail as the user, or change the user's preference settings.

Vulnerability Details:

[NT] Session Token Remains Valid After Logout in IBM Lotus Domino Web Access

When a Lotus DWA user logs in, a cookie called "LtpaToken" is set into the browser and is used throughout the session to uniquely identify the user. When a user logs out of DWA, the cookie is cleared from the browser, but this action has no effect on the server. The token eventually expires on the server after some configurable amount of time. A user who explicitly logs out of DWA may have a false sense of security. The LtpaToken cookie in his browser is deleted, but the token is still valid from the server's perspective and can be used by an attacker if he can discover it. Best practices in web application security would call for the LtpaToken to be invalidated/destroyed at logout time. Note that the vulnerability described here was observed with Session authentication under the Domino Web Engine tab set to "Multiple Servers (SSO)". The same behavior may occur with the "Single Server" configuration as well, but this was not tested.

The "LtpaToken" described here is a component in IBM's Lightweight Third-Party Authentication (LTPA) technology. The LTPA technology was designed to be a defacto standard across the IBM product family. LTPA is used in both IBM WebSphere and Lotus Domino products and allows for single sign-on across physical servers. For example, Domino can recognize and accept LTPA tokens created by WebSphere. For more information, please see the IBM redpaper at <http://www.redbooks.ibm.com/redpieces/pdfs/redp4104.pdf>

Mitigating Factors:

Keeping the LtpaToken confidential is critical to mitigating this issue. An attacker must be able to discover a valid LtpaToken before it expires. Because the LtpaToken is sent with each request, Lotus DWA should be deployed as a secure application. This means an SSL certificate should be installed on the server so that encrypted (https) communication between the browser and the server occurs.

Cross-site scripting (XSS) is a common application-level attack that can be used to steal cookies such as LtpaToken. Running the application under SSL does not hinder XSS attacks. Fortunately, Lotus Domino includes a module called Active Content Filter that is highly effective at removing potentially harmful scripts in e-mail messages. Active Content Filtering should be turned on.

Finally, the overall risk level can be lowered by enabling an idle session timeout in addition to the absolute expiration time. Ideally, from an application security perspective, the idle (inactivity) timeout would be much smaller than the absolute expiration. Be aware that the increased security from having small timeout values may negatively affect end-user satisfaction in the application.

Recommendations:

IBM recommends running Lotus DWA run under SSL and using a token expiration time of 30 minutes.

[NT] Session Token Remains Valid After Logout in IBM Lotus Domino Web Access

Please see IBM technote #1245589:

<http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21245589>

<http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21245589>

ADDITIONAL INFORMATION

The information has been provided by

<mailto:dave.ferguson@xxxxxxxxxxxxxxxxxxxxxx> Dave Ferguson.

=====

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@xxxxxxxxxxxxxxxxxx

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

=====

=====

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.