

## IBM Lotus Domino Web Access 7.0.1

- This document contains a detailed vulnerability and attack overview for Lotus Domino Web Access (DWA) 7.0.1
- As well, this document provides both vulnerability details and mitigating factors, concluding with recommended actions from the FishNet Security Vulnerability Research Team.

### CORPORATE BACKGROUND

FishNet Security is a nationally respected information security solutions provider. FNS expertise includes information security strategy, continuous risk and application assessment, planning, implementation, management, training and support -- enabling businesses to meet their unique security needs. Since 1996, FNS has offered information security services and products to global enterprises, government agencies, and small-medium sized businesses. For more information about FishNet Security, please visit us at [www.fishnetsecurity.com](http://www.fishnetsecurity.com).

### ENGINEERING AND CONSULTING EXPERTISE

FishNet Security offers a technical staff with experience, training, and industry certifications such as Check Point Certified Security Expert, Cisco Certified Internetwork Engineer (CCIE), Certified Information Systems Security Professional (CISSP), Microsoft Certified System Engineer, and more. Our engineers are certified in industry-leading security product lines, and in the networking, operating system, and routing foundations that underscore successful implementations. Our security consultants offer a high level of expertise in assessing and auditing applications and software systems for vulnerabilities and compliance issues.

### FISHNET SECURITY VULNERABILITY RESEARCH TEAM

The FishNet Security Vulnerability Research Team is comprised of highly technical engineers and consultants and is designed to be flexible to meet the varying needs of FishNet Security and our clients. The following individuals participated in the vulnerability research on this project:

David Ferguson, Security Consultant  
Vulnerability discovery and threat analysis  
Office: +1 (816) 421.6611  
Email: [dave.ferguson@fishnetsecurity.com](mailto:dave.ferguson@fishnetsecurity.com)

Jake Reynolds, Senior Security Engineer  
Additional threat analysis  
Office: +1 (816) 421.6611  
Email: [jake.reynolds@fishnetsecurity.com](mailto:jake.reynolds@fishnetsecurity.com)

Arian Evans, Senior Security Engineer  
Additional threat analysis  
Office: +1 (816) 421.6611  
Email: [arian.evans@fishnetsecurity.com](mailto:arian.evans@fishnetsecurity.com)

## IBM Lotus Domino Web Access 7.0.1

### EXECUTIVE SUMMARY

#### Vulnerability Overview:

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.

#### 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.

### TECHNICAL DETAIL

#### Vulnerability Detail:

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 provides a single sign-on mechanism across servers. For example, Domino can recognize and accept LTPA tokens created by WebSphere. For more information, please see the IBM redpaper.

#### 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.

## IBM Lotus Domino Web Access 7.0.1

### RECOMMENDED ACTIONS

See "Mitigating Factors" above. In addition, IBM recommends include running Lotus Domino Web Access run under SSL and using a token expiration time of 30 minutes.

Please see IBM technote #1245589:  
<http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21245589>

### Contact

You can reach the author of this advisory at: [dave.ferguson@fishnetsecurity.com](mailto:dave.ferguson@fishnetsecurity.com)  
Media professionals, please contact Jon Forbis at (888) 732.9406 or by email at [jon.forbis@fishnetsecurity.com](mailto:jon.forbis@fishnetsecurity.com)