

SECURITY ADVISORY

June 2008

Direct Web Remoting – Cross-Site Scripting on Error Page



Table of Contents

The Security Research Team.....	2
Issue History	3
Issue Description	4
Issue Impact	4
Affected Components	4
Exploit	4
Mitigation	4
CVSS Base Score	4

Copyright and Disclaimer

The information in this advisory is Copyright 2008 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team/Peter Österberg.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

Issue History

This document has been updated to the present version as information has been received from various external sources.

- Oct 2007 Issue originally discovered within the DWR community,
<https://dwr.dev.java.net/servlets/ReadMsg?listName=users&msgNo=10475>
- May 14 2008 Issue publicly discovered by Peter Österberg
- May 14 2008 Vendor was contacted
- May 15 2008 Vendor reports back that the issue is corrected as of version 2.0.2
- June 17 2008 Disclosure date

THIS DOCUMENT IS TENTATIVELY SCHEDULED FOR PUBLIC RELEASE VIA THE FORTCONSULT WEBSITE AND SECURITY MAILING LISTS IN June 2008.

Issue Description

DWR generated javascripts are commonly generated under a folder named
.../dwr/interface/javascript.js.

An error message will pop up if a user navigates to an URL under this folder that doesn't exist.

Example: <http://somedomain/dwr/interface/nonexistent.js>.

The error will say something similar to: "No class by name: nonexistent"

The generation of this error message does not sanitize the *nonexistent* part. This makes it possible to post javascript in the URL. This javascript will be part of the generated error page and will, if properly encoded, execute in the users browser.

Issue Impact

The vulnerability could possibly be used to steal session cookies from a user.

Affected Components

Direct Web Rendering (DWR – Easy Ajax for JAVA) – <http://getahead.org/dwr>

Version: 2.0.1, other versions might be affected as well

Exploit

Navigate your web browser to [http://somesite/dwr/interface/nopage<script>alert\(123\)</script>](http://somesite/dwr/interface/nopage<script>alert(123)</script>)

Success

The above example will work FireFox browsers, it normally has to be URL-encoded to work properly in an Internet Explorer browser.

Mitigation

Upgrade to version 2.0.2

and / or

Use a custom made error page and don't let DWR to generate the error page as it does in its default behavior.

CVE-reference

CVE-2008-2740

CVSS Base Score

FortConsult has used the online CVSS calculator found at <http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx> to calculate these scores.

BASE SCORE: 3.5

Metrics:

Access Vector: Remote

Access Complexity: Low

Authentication: Not Required

Confidentiality Impact: Partial

Integrity Impact: None

Availability Impact: None

Impact Bias: Confidentiality