

SECURITY ADVISORY

February 2009

FotoWeb Multiple Cross-Site Scripting Vulnerabilities



Discovered in February 2009 by FortConsult's Security Research Team/Stelios Tigkas

This document contains proprietary and confidential information. An informal, nonbinding understanding exists between FotoWare and FortConsult that, for the safety of our customers and other users, the details of this advisory will not be made public until February 2009, when FotoWare releases updated versions of the software together with information on how to avoid the security risks described in this advisory. Please DO NOT forward this document to ANYONE, in any way whatsoever.

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/Stelios Tigkas

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.

December 2008: Issue discovered by Stelios Tigkas

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

Issue Description

There are two Cross-Site Scripting Flaws in the FotoWeb Application:

- The Hidden Parameter "s" is vulnerable. The "s" parameter is used in several different pages of the Application (including "Login.fwx") and seems to be used for redirection purposes
- The "Search" Parameter in "Grid.fwx" is vulnerable. The event is triggered only if the search result is not null. Therefore, it is necessary to append an additional parameter that returns at least some results to trigger the XSS.

Issue Impact

This vulnerability can be used for Credential theft.

Affected Components

FotoWeb Version 6.0 (Build 273). Other versions may be affected as well.

Exploit

The issues can be triggered as follows:

[<script>alert\("0wn3d"\)</script>](http://www.somesite.dk/fotoweb/cmdrequest/Login.fwx?s=)
[http://www.somesite.dk/fotoweb/Grid.fwx?&search=<script>alert\("0wn3d"\)</script> and \(FYFT contains\(JPEG\)\)](http://www.somesite.dk/fotoweb/Grid.fwx?&search=<script>alert()

Mitigation

As a temporary workaround whilst on standby for the vendor to release a fix or an updated version of FotoWeb, attempt your own input validation at the Firewall Layer, if possible. You could also use some other custom-made input validation solution.

CVE-reference

TBC

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: 4.3

Metrics:

Access Vector: Remote

Access Complexity: Medium

Authentication: Not Required

Confidentiality Impact: None

Integrity Impact: Partial

Availability Impact: None