

Re: [Full-Disclosure] ColdFusion cross-site scripting security vulnerability of an error page

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-09/1393.html>

From: morning_wood (se_cur_ity_at_hotmail.com)

Date: 09/23/03

To: <sec@v23.org>, <full-disclosure@lists.netsys.com>

Date: Tue, 23 Sep 2003 11:49:07 +0530

they (Macromedia) downplayed this..

<http://nohackers.org/pipermail/Oday/2003-June/000028.html>

<http://nohackers.org/pipermail/Oday/2003-June/000029.html>

<http://nohackers.org/pipermail/Oday/2003-June/000030.html>

as i am sure they will do with yours, as they think XSS is not a security issue.

D. Werner

CTO E2 Labs Infosec

<http://e2-labs.com>

----- Original Message -----

From: <sec@v23.org>

To: <full-disclosure@lists.netsys.com>

Sent: Tuesday, September 23, 2003 10:39 AM

Subject: [Full-Disclosure] ColdFusion cross-site scripting security vulnerability of an error page

> *ColdFusion cross-site scripting security vulnerability of an error page*

>

> > *The outline of vulnerability*

>

> *Macromedia's ColdFusion can display the various information about an error at the time of error occurred.*

> *There is information transmitted from a client machine like "Referer".*

> *ColdFusion displays the information as it is.*

> *An attacker can execute a script on victim's browser by preparing for*

> *WEB the link which embedded arbitrary scripts.*

>

>

> > *User's risk*

>

> *The user who accesses a vulnerable server has a risk that forced to*

> *execute the arbitrary javascript and HTML code which the attacker*

> *embedded.*

Full-Disclosure: Re: [Full-Disclosure] ColdFusion cross-site scripting security vulnerability of an error page

- > *Risks of being assumed are below.*
- > *session high-jack (by stolen cookie)*
- > *page defacement by embedded html tags.*
- > *etc.*
- > *It is insecure to store critical information (such as personal*
- > *information) without encryption in cookie. Such a poor*
- > *application will make risk bigger when session-highjack occurs.*
- >
- >
- >> *The range of influence*
- >
- > *This problem is contained in the error page of all versions of*
- > *ColdFusion.*
- > *This problem does not occurred when ColdFusion's error page does not*
- > *include the contents transmitted from client machines (such as "Referer"*
- > *).*
- >
- >
- >> *About vulnerability*
- >
- > *In Cold Fusion, an error screen is displayed at the time of error*
- > *occurred.*
- > *It is possible to display the contents transmitted from the client*
- > *machine (#error.HTTPReferer#) as it is.*
- > *When the code for an attack is contained in the contents to display, a*
- > *cross-site scripting attack can be executed.*
- >
- > *For example, the script will be executed when the script for an attack*
- > *is embedded by "Referer" in #error.HTTPReferer#, and an error screen is*
- > *displayed.*
- > *The same problem exists in the #error.QueryString# .*
- >
- >
- >> *Sample attack*
- >
- > *User using Cold Fusion of the site A (www.CFtestA.com).*
- > *The method of stealing cookie is bellow.*
- >
- > *1. An attacker creates the page B (www.atack_testA.com/cf.html) with the*
- > *link to the site A.*
- > *2. Next, after considering the invitation complaint which is easy to*
- > *guide victims, such as present collection, to another page, the link to*
- > *Page B is attached.*
- > *A code for an attack is embedded into this link, that code remains as*
- > *"Referer" information as it is, and when it clicks the link to the site*
- > *A which has a victim in Page B, it will be executed.*
- > *Example: alert*
- > *(document.cookie) </script>"> GET PRIZE! HERE'S PRIZE LINKS!*
- >
- > *When cookie is published in site A, it can steal by this method.*
- > *In addition, cf.html does not need to have the mechanisms (CGI etc.).*

Full-Disclosure: Re: [Full-Disclosure] ColdFusion cross-site scripting security vulnerability of an error page

- > *The code below "?" is disregarded. cf.html is only displayed.*
- > *However, an attack becomes possible in order for "?" or subsequent ones*
- > *to remain in "Referer" as it is.*
- > *By changing the code embedded by the same method, it becomes possible to*
- > *execute arbitrary codes.*
- >
- >
- >
- > >> *Solution*
- >
- > *The patch corresponding to this problem is distributed at Macromedia.*
- > *A patch can come to hand by Following URL.*
- > *URL of http://www.macromedia.com/devnet/security/security_zone/mpsb03-06.html*
- > *html*
- > *Moreover, you should not use an error page which displays the contents*
- > *transmitted from a client machine as it is irrespective of the existence*
- > *of patch application.*
- > *Although it may be necessity at the debugging time, it is dangerous with*
- > *real operation environment.*
- >
- > *T.Hara , Scan Security Wire <http://www.scan-web.com/>.*
- > *<http://www.scan-web.com/jvi/index.cgi>*
- >
- >
- >
- >
- > _____
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*
- >

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>