

Securiteam: [NEWS] Security Issue Found with Customized Login Pages for Oracle SSO

# [NEWS] Security Issue Found with Customized Login Pages for Oracle SSO

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0093.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 03/31/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 31 Mar 2004 10:26:11 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Security Issue Found with Customized Login Pages for Oracle SSO

---

## SUMMARY

A vulnerability in Oracle SSO's mechanism allows a customized Sign On page to be built by administrators. A vulnerability in the sample pages (used by most administrators) allows an attacker to send a special URL to the victim (Oracle user) that once it is opened, all sensitive information (Usercode, Password, etc) can be made to travel to the attacker.

## DETAILS

Oracle has a Single Sign-on application called OSSO.

Among others, it has a web based login form. This form can be customized as explained in "Oracle 9iAS Single Sign-on Administrators Guide, Release 2(9.0.2), Part No. A96115-01". In this document, a sample login form is published (section 8).

The problem with this login form is that unauthorized persons are able to gain access to the supplied usercode and password. This is done by tricking a valid user into opening a URL that is the real URL of the customized SSO login page with a modified URL parameter.

## Securiteam: [NEWS] Security Issue Found with Customized Login Pages for Oracle SSO

The problem is that the attack makes use of the real login page. Thus, if users check host certificates only, they will not be able to detect that they are being tricked. Also, after logging in, they can be redirected to the proper application on the intended system to hide the fact that usercode and password have been stolen.

Note that the problem is a design problem in the way custom login pages must be implemented, not a problem with a sample script.

### Impact:

Users can accidentally reveal their SSO usercode/password combination to unauthorized persons.

### Vendor response:

Oracle came with the following solution:

The p\_submit\_url value in the customized login page can be hard-coded. This will mitigate this issue since it will not be an input value to the page anymore. The p\_submit\_url URL value in the 902 SSO server is in the following format:

`http(s)://sso_host:port/pls/orasso/orasso.wwsso_app_admin.ls_login`

### Recommendation:

We recommend implementing the proposed solution.

Of course, we hope that Oracle will update its documentation as well such that the p\_submit\_url parameter will be removed from all example code.

## ADDITIONAL INFORMATION

The information has been provided by  
<mailto:advisories@madison-gurkha.com> Guido van Rooij (Madison Gurkha)  
and Arjan de Vet (Madison Gurkha).

The original article can be found at:

<<http://www.madison-gurkha.com/advisories/MG-2004-01.txt>>  
<http://www.madison-gurkha.com/advisories/MG-2004-01.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,

Securiteam: [NEWS] Security Issue Found with Customized Login Pages for Oracle SSO  
loss of business profits or special damages.