



**CYBSEC S.A.**  
[www.cybsec.com](http://www.cybsec.com)

**Advisory Name:** Oracle Forms Unauthenticated Cross-Site Scripting

**Vulnerability Class:** Cross-Site Scripting

**Release Date:** 2008-01-16

**Affected Applications:**

- Oracle Forms 10.1.2.2

**Affected Platforms:**

- Oracle Forms 10.1.2.2

**Local / Remote:** Remote

**Severity:** Medium

**Author:** Mariano Nuñez Di Croce

**Vendor Status:**

- Confirmed. Updates Released.

**Reference to Vulnerability Disclosure Policy:**

[http://www.cybsec.com/vulnerability\\_policy.pdf](http://www.cybsec.com/vulnerability_policy.pdf)

**Product Overview:**

“Oracle Forms, a component of the Oracle Developer Suite, is Oracle's long-established technology to design and build enterprise applications quickly and efficiently.”

**Vulnerability Description:**

When accessing an application based on Jinitiator, it is possible to trigger a XSS vulnerability, as the *frmservlet* servlet fails to validate the parameter *ifcmd*, allowing the inclusion of Javascript code in the returned HTML page.

**Impact:**

Exploitation of this vulnerability would allow an attacker to craft a special link that, when accessed by a regular user of the application, will enable him to execute arbitrary Javascript code in the browser of the affected user.

**Solutions:**

Oracle has released fixes in the January 2008 CPU.

More information in <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html>

**Vendor Response:**

- 2007-07-16: Initial Vendor Contact.
- 2007-07-24: Vendor Confirmed Vulnerability.
- 2007-08-24: Vendor Confirmed Vulnerability was fixed.
- 2008-01-15: Vendor Releases Critical Patch Update.
- 2008-01-17: Advisory Public Disclosure.

**Contact Information:**

For more information regarding the vulnerability feel free to contact the author at [mnunez <at> cybsec <dot> com](mailto:mnunez@cybsec.com).

**About CYBSEC S.A. Security Systems**

Since 1996 CYBSEC S.A. is devoted exclusively to provide professional services specialized in Computer Security. More than 150 clients around the globe validate our quality and professionalism.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information regarding CYBSEC: [www.cybsec.com](http://www.cybsec.com)