



**CYBSEC**<sup>S.A.</sup>  
Security Systems

**CYBSEC S.A.**

[www.cybsec.com](http://www.cybsec.com)

**Advisory Name:** Arbitrary file overwrite in Documentum Administrator / Documentum Webtop

**Vulnerability Class:** Arbitrary file overwrite

**Release Date:** 2008-02-05

**Affected Applications:**

- Documentum Administrator version 5.3.0.313
- Documentum Webtop version 5.3.0.317
- Other applications and versions may also be affected

**Affected Platforms:**

- Windows 2003 Server - Standard Edition
- Apache Tomcat 5.0.28
- Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2\_05-b04)
- Other platforms may also be affected

**Local / Remote:** Remote

**Severity:** High

**Researcher:** Pablo Gaston Milano

**Vendor Status:** Confirmed. Updates Released.

**Reference to Vulnerability Disclosure Policy:**

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

## **Vulnerability Description:**

Documentum Administrator and Documentum Webtop were found to be vulnerable to arbitrary file overwrite, by specifying an arbitrary filename attribute to the "dmclTrace.jsp" page. It is also possible to control the contents of the overwritten file, which could allow the remote upload and execution of arbitrary code in the context of the user running the application server.

## **Exploit:**

A fully functional exploit was developed and was provided to the vendor for analysis.

## **Impact:**

Exploitation of this vulnerability would allow an attacker to overwrite arbitrary files on the server filesystem. This could be used to upload and execute arbitrary code in the context of the user running the application server.

## **Solution:**

The vendor reported that this vulnerability was fixed in SP4 and later.

## **Vendor Response:**

- 2007-12-17: CYBSEC contacted Vendor.
- 2007-12-17: Vendor first response.
- 2008-01-04: Vendor confirmed vuln is fixed in latest SP.
- 2008-01-30: CYBSEC informed the vendor the disclosure plan.
- 2008-02-05: Advisory Public Disclosure.

## **Contact Information:**

For more information regarding the vulnerability feel free to contact the researcher at pmilano <at> cybsec <dot> 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, please visit [www.cybsec.com](http://www.cybsec.com)

(c) 2008 - CYBSEC S.A. Security Systems