



**Advisory Name:** SAP sapstartsrv Denial of Service

**Vulnerability Class:** Denial of Service

**Release Date:** 12-10-2009

**Affected Applications:** SAP Kernel 6.40, 7.00, 7.01, 7.10, 7.11 and 7.20. Other versions may also be affected.

**Affected Platforms:** All SAP platforms running sapstartsrv

**Local / Remote:** Remote

**Severity:** Medium

**Researcher:** CYBSEC-Labs Team

**Vendor Status:** Confirmed. Updated Released

**Reference to Vulnerability Disclosure Policy:** [http://www.cybsec.com/vulnerability\\_policy.pdf](http://www.cybsec.com/vulnerability_policy.pdf)

**Vulnerability Description:**

In SAP instances, the sapstartsrv service provides a Web SAP Management Console interface for remote administration. Due to a failure in the processing of specially crafted requests, it is possible to remotely shutdown the associated process.

**Proof of Concept:**

A PoC was developed and was provided to the vendor for analysis.

**Impact:**

Exploitation of this vulnerability would allow a remote attacker to deny access to the SAP Management Console, interfering with the administrators' operation.

**Solution:**

SAP has released patches to address this vulnerability. Affected customers should apply the patches immediately. More information can be found on SAP Note 1302231.

**Vendor Response:**

2009-02-02: CYBSEC contacted Vendor.



2009-02-12: Vendor confirmed Vulnerability.

2009-02-13: Vendor Releases Patches.

2009-12-10: Advisory Public Disclosure.

### **Contact Information:**

For more information regarding the vulnerability feel free to contact the CYBSEC Labs Team (cybseclabs <at> cybsec <dot> com), who will provide any further information that may be required.

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

CYBSEC is a leading Information Security company with more than 13 years of expertise. More than 350 clients in Latin America, Europe and USA guarantee our commitment.

Our Professional Services includes SAP Security, Secure Configuration, Web Applications Security, Security Audit (SOX, PCI and ISO 27001) and Penetration Testing.

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, please visit [www.cybsec.com](http://www.cybsec.com)

(c) 2009 - CYBSEC