

**Advisory Name:** SQL Command Exec in Hipergate

**Vulnerability Class:** SQL Command Exec

**Release Date:** 2010-02-02

**Affected Applications:** Confirmed in Hipergate 4.0.12. Other versions may also be affected.

**Affected Platforms:** Multiple

**Local / Remote:** Remote

**Severity:** High – CVSS: 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

**Researcher:** Nahuel Grisolia

**Vendor Status:** Still Vulnerable – No Patch Available at the moment

**Vulnerability Description:**

A vulnerability has been discovered in Hipergate, which can be exploited by malicious people to conduct SQL Command Execution Attacks.

The vulnerability is confirmed in version 4.0.12. Other versions may also be affected.

**Proof of Concept:**

<http://x.x.x.x:8080/hipergate/admin/sql.htm>

**Impact:** Execute arbitrary SQL queries.

**Solution:** Maybe in Build 5.5 (Future Release, information provided by the vendor)

**Vendor Response:** Last Contact on January 12, 2010. They said that no more patches would be provided since Build 5.5 will be released soon.

**Contact Information:**

For more information regarding the vulnerability feel free to contact the researcher at **nahuel.grisolia <at> gmail <dot> com**