Advisory Name: Reflected Cross-Site Scripting (XSS) in Hipergate

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

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: Medium – CVSS: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Researcher: Nahuel Grisolía

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

Vulnerability Description:

A reflected Cross Site Scripting vulnerability was found in Hipergate 4.0.12, because the application fails to sanitize user-supplied input. Any logged-in user can trigger the vulnerability.

Proof of Concept:

http://x.x.x.x:8080/hipergate/common/errmsg.jsp?title=%3Cscript%3Ealert%28%22titleXSS%22%29;%3C/script%3E&desc=%3Cscript%3Ealert%28%22descXSS%22%29;%3C/script%3E&resume=_back

Script pwd_errmsg.jsp is also affected.

Impact:

An affected user may unintentionally execute scripts or actions written by an attacker. In addition, an attacker may obtain authorization cookies that would allow him to gain unauthorized access to the application.

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