**Advisory Name:** Multiple Reflected Cross-Site Scripting (XSS) in McAfee Email Gateway (formerly IronMail)

**Vulnerability Class:** Reflected Cross-Site Scripting (XSS)

**Release Date:** Tue Apr 6, 2010

**Affected Applications:** Secure Mail (Ironmail) ver.6.7.1

**Affected Platforms:** FreeBSD 6.2 / Apache-Coyote 1.1

**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:** Official Patch Released. Install McAfee Email Gateway 6.7.2 Hotfix 2.

**Reference to Vulnerability Disclosure Policy**: http://www.cybsec.com/vulnerability_policy.pdf

## Vulnerability Description:

Multiple Reflected Cross Site Scripting vulnerabilities were found in Ironmail's Web Access console, because the application fails to sanitize user-supplied input. The vulnerabilities can be triggered by any logged-in user.

## Proof of Concept:

* Parameters like “queueMsgType” and “QtnType” in queuedMessage.do are not properly sanitized. To reproduce the XSS, simply paste the following URL with an authorized user:

https://XXX.XXX.XXX.XXX:XXXXX/admin/queuedMessage.do?method=getQueueMessages&queueMsgType=<script>alert("XSS");</script>&QtnType=9

Other parameters might also be 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 Web console.

**Solution:** Official Patch. Refer to https://kc.mcafee.com/corporate/index?page=content&id=SB10008

**Vendor Response:**

Dec 1, 2009 / First Contact.
Dec 1, 2009 to Apr 5, 2010 / The Vendor has been working very hard on this. Issue fixed.
Apr 6, 2010 / Vulnerability went Public.

**Contact Information:**

For more information regarding the vulnerability feel free to contact the researcher at
ngrisolia <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