Advisory Name: Denial of Service in McAfee Email Gateway (formerly IronMail)

Vulnerability Class: Denial of Service

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: 4.6 (AV:L/AC:L/Au:S/C:N/I:N/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:

Users inside the CLI can run some kind of "Fork Bomb" in order to saturate system resources because of an insecure ulimit value.

Exploit:

* In order to run the DoS, follow the steps below:

[Secure Mail]: command rbash –noprofile
[Secure Mail]: :(){:|:&};:

Impact:

Denial or disruption of service attacks affect the availability of data, services, and network elements.

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
(c) 2010 - CYBSEC S.A. Security Systems