```
************************************************************
*                                                          *
*           goSecurity - Advisory 2010111902               *
*                                                          *
************************************************************

Software:           IceWarp Mail Server
Date:               06 Dec. 2010
Affected Versions:  10.1.3 (partially), 10.2.0

************************************************************
*   Multiple XSS vulnerabilities in IceWarp Webclient      *
************************************************************

Summary
-------
IceWarp Webclient is prone to multiple Cross-Site
Scripting (non-persistent and persistent) vulnerabilities.
All of them must be triggered by HTTP-POST requests.

************************************************************

Details
-------
Input passed via the following parameters is not properly
sanitised before being returned to the user. This can be
exploited to execute arbitrary HTML and script code in a
user's browser session in context of an affected site.

File:       http[s]://host/admin/login.html
Parameter:  username
Type:       persistent XSS
Version:    10.2.0

File:       http[s]://host/webmail/basic/
Parameter:  _dlg[captcha][controller]
Type:       non-persistent XSS
Version:    10.1.3, 10.2.0 (possibly all 10.x versions <=10.2.0)

File:       http[s]://host/webmail/basic/
Parameter:  _dlg[captcha][action]
Type:       non-persistent XSS
Version:    10.1.3, 10.2.0 (possibly all 10.x versions <=10.2.0)

File:       http[s]://host/webmail/basic/
Parameter:  _dlg[captcha][uid]
Type:       non-persistent XSS
Version:    10.1.3, 10.2.0 (possibly all 10.x versions <=10.2.0)

File:       http[s]://host/webmail/
Parameter:  password
Type:       non-persistent XSS
Version:    10.2.0

************************************************************

Solution
--------
Upgrade to Version 10.2.1
```

****

Credits

Ron Ott - GO OUT Production GmbH
Mike Schneider - GO OUT Production GmbH
Thomas Wittmann - Wittmann Security Consulting

****

Timeline (CET)

18/11/10   Vulnerabilities discovered and confirmed with
            multiple installations of IceWarp Webclient
            10.1.3 and 10.2
19/11/10   First contact with vendor
23/11/10   Confirmed by vendor
24/11/10   Fixed by vendor
29/11/10   Customer information by vendor

****