YGN ETHICAL HACKER GROUP

Security Advisory

GMAIL-LITE SHELL CODE EXECUTION Vulnerability

Discovered by: br0
Date: March 2008
URL: All Gmail-Lite hosting sites which enable file uploading feature
Vulnerability Type: **SHELL CODE EXECUTION**
Risk: **high**
Threats: Entire 0wnage

Note:

Gmail-Lite lets us upload our desired files when we mail to our friends. It doesn't even restrict files types. In this case, an attacker can upload backdoor php scripts to the server. There, he can run his desired shell codes to do anything he wants.

Proof-Of-Vulnerability:

Fix:

Just create .htaccess file with contents below and place it on the uploads folder to disable running malicious scripts. The following .htaccess. will save you:

```
AddHandler cgi-script .php .php3 .php4 .phtml .pl .py .jsp .asp .htm .shtml .sh .cgi
Options –ExecCGI –indexes

Order allow, deny
Deny from all
```

Disabling execution of these files could give you an extra layer of protection.