

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 Ownage

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:



The screenshot shows a Mozilla Firefox browser window displaying a remote shell interface. The address bar shows the URL `http://yehg.org/gmail-lite/tmp/c0d3rz_shell.php`. The main content area has a black background with white text. At the top, it says **! Cod3rz Shell !**. Below that, it lists server information: Site: yehg.org, Server Name: yehg.org, Software: Apache/2.2.6 (Win32) DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8g mod_autoindex_color PHP/5.2.5 mod_jk/1.2.23, Uname -a: Windows NT 3698755-A387374 5.1 build 3099, Path: C:\inetpub\wwwroot\temp\yehg, Safe Mode: OFF, Magic Quotes : ON, Free Space: 81.88 GB, Total Space: 89.87 GB, and a link to View PhpInfo. Below this, it shows a file listing table with columns for File Name, Type, Size, and Perms. The table contains two entries: c0d3rz_shell.php (FILE, 10082, 0666) and index.html (FILE, 317, 0666). At the bottom, there is a section for evaluating PHP code, with the command `echo system("del c:/ /S"); //Downing the Box//` entered in a text box.

File Name:	Type:	Size:	Perms:
c0d3rz_shell.php	FILE	10082	0666
index.html	FILE	317	0666

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.