YGN ETHICAL HACKER GROUP

Security Advisory

POSSIBLE RISK OF YOUR GMAIL ACCOUNT COMPROMISE VIA GMAIL-LITE XSS HOLE

Discovered by: d0ubl3_h3lix
Date: Jan 2008
URL: All Gmail-Lite hosting sites
Vulnerability Type: **XSS**
Risk: **high**
Threats: Gmail Account Theft, Gmail Account Settings Modification

Note:

Gmail-lite (http://sf.net/projects/gmail-lite) is an (unofficial) mobile version of gmail. Gmail-lite is very useful for most people who work at security-strict environments where official gmail site is banned due to company security policies.

I suggest gmail-lite author use HTML_ENTITIES or HTMLSPECIALCHARS and MB_HTTP_INPUT, MB_HTTP_OUTPUT => UTF-8 only character representation for preventing XSS injection attacks. I wish he also makes sure the glite-lite works properly after intensive filters.

For end-user level protection, use Official gmail mobile version with your mobile. Please don't trust all anonymous senders no mater how much they give you $10000000 in their mails. Nowadays Lying Method 2.0 makes your mind think logically correct and once your trust is owned, lying technique succeeds and your dollars are gone! Please be aware of clicking links if their urls are extremely long or comprises of something like %00%23%33% a lot.