

Squirrelmail

Martijn Brinkers discovered cross-site scripting vulnerabilities in the *mailto* parameter of *webmail.php*, the *session* and *delete_draft* parameters of *compose.php*, and through a shortcoming in the magicHTML filter. An attacker could abuse these problems to execute malicious JavaScript in the user's webmail session. (CVE-2006-6142)

Debian reference: DSA-1241-1

Suse reference: SUSE-SR:2006:029

madwifi-ng

The madwifi-ng Atheros Wireless LAN card driver is subject to a remotely exploitable stack buffer overflow, which could lead to either code execution or at least a denial of service (kernel crash).

A physical local attacker (within WLAN range) has to provide a malicious access point which the card tries to associate with to be able to effect this attack. The madwifi-ng Atheros Wireless

LAN card driver is subject to a remotely exploitable stack buffer overflow.

To succeed with this attack, a physical local attacker (within WLAN range) has to provide a malicious access point, which the card tries to associate with. (CVE-2006-6332)

Gentoo reference: GLSA 200612-09

Suse reference: SUSE-SA:2006:074

Xine

xine-lib is vulnerable to a buffer overflow in the Real Media input plugin, which could lead to the execution of arbitrary code.

xine is a portable and reusable multimedia playback engine. xine-lib is xine's core engine. A possible buffer overflow has been reported in the Real Media input plugin. (CVE-2006-6172) An attacker could exploit this by enticing a user into loading a specially crafted stream with xine or an application using xine-lib. This can lead to a Denial of

Service and possibly the execution of arbitrary code with the rights of the user running the application.

Gentoo reference: GLSA 200612-02

Slackware reference: SSA:2006-357-05

Suse reference: SUSE-SR:2006:028

Ruby

Ruby is a dynamic, open source programming language with a focus on simplicity and productivity.

The *read_multipart* function of the CGI library shipped with Ruby (*cgi.rb*) does not properly check boundaries in MIME multipart content. (CVE-2006-5467) The vulnerability can be exploited by sending the *cgi.rb* library a crafted HTTP request with multipart MIME encoding that contains a malformed MIME boundary specifier. Successful exploitation of the vulnerability causes the library to go into an infinite loop.

Gentoo reference: GLSA 200612-21

Ubuntu reference: USN-394-1

Linux Magazine Exclusive

