

# [Full-disclosure] MDKSA-2005:120 – Updated mozilla-firefox packages fix multiple vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-07/0271.html>

---

**From:** Mandriva Security Team ([security\\_at\\_mandriva.com](mailto:security_at_mandriva.com))

**Date:** 07/14/05

To: [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)

Date: Wed, 13 Jul 2005 21:50:44 -0600

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

---

## Mandriva Linux Security Update Advisory

---

Package name: mozilla-firefox  
Advisory ID: MDKSA-2005:120  
Date: July 13th, 2005

Affected versions: 10.2

---

### Problem Description:

A number of vulnerabilities were reported and fixed in Firefox 1.0.5 and Mozilla 1.7.9. The following vulnerabilities have been backported and patched for this update:

In several places the browser UI did not correctly distinguish between true user events, such as mouse clicks or keystrokes, and synthetic events generated by web content. The problems ranged from minor annoyances like switching tabs or entering full-screen mode, to a variant on MFSA 2005-34 Synthetic events are now prevented from reaching the browser UI entirely rather than depend on each potentially spoofed function to protect itself from untrusted events (MFSA 2005-45).

Scripts in XBL controls from web content continued to be run even when Javascript was disabled. By itself this causes no harm, but it could be combined with most script-based exploits to attack people running

vulnerable versions who thought disabling javascript would protect them. In the Thunderbird and Mozilla Suite mail clients Javascript is disabled by default for protection against denial-of-service attacks and worms; this vulnerability could be used to bypass that protection (MFSa 2005-46).

If an attacker can convince a victim to use the "Set As Wallpaper" context menu item on a specially crafted image then they can run arbitrary code on the user's computer. The image "source" must be a javascript: url containing an eval() statement and such an image would get the "broken image" icon, but with CSS it could be made transparent and placed on top of a real im