

By: [Bartolab](#) 2007 Security and Search Engines Editor

[Users Urged to Install the Latest Mozilla Thunderbird Patch](#)

In order to remain protected while using the application

Thunderbird, the well-known email client designed by Mozilla, must be updated as soon as possible in order to keep the computer protected, the developers of the application said a few days ago. Several vulnerabilities have been discovered in the program, so the installation of the latest patch is almost a must have. According to the reports, most Thunderbird versions contain the glitch, with a single exception: the 1.5.0.14 release, which comes to correct the issue. One of the email client vulnerabilities has been created by the JavaScript support, which could be used by an attacker who managed to exploit the flaw and to compromise an affected system, security company Secunia wrote in an advisory. Secunia rated the vulnerabilities as highly critical and also urged the users to install the latest release as soon as possible. Mozilla has already released a report to confirm the vulnerabilities, adding that the updates are also supposed to improve the stability of both Firefox and Thunderbird. "Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code", Mozilla mentioned. "Thunderbird shares the browser engine with Firefox and could be vulnerable if JavaScript were to be enabled in mail. This is not the default setting and we strongly discourage users from running JavaScript in mail. Without further investigation we cannot rule out the possibility that for some of these an attacker might be able to prepare memory for exploitation through some means other than JavaScript such as large images." Just like usual, you can download the latest version of Mozilla Thunderbird straight from our website, using the following [link](#). If you want to read more information about the recent Thunderbird update, you can check the information provided by Mozilla available [here](#).