

# Flaw found in Firefox

By *srlinuxx*

Created 05/04/2005 - 11:07pm

Submitted by srlinuxx on Tuesday 5th of April 2005 11:07:21 PM Filed under [Security](#) [1]

Firefox versions 1.0.1 and 1.0.2 contain the vulnerability, the security information company said in an advisory on Monday. The flaw stems from an error in the JavaScript engine that can expose arbitrary amounts of heap memory after the end of a JavaScript string. As a result, an exploit may disclose sensitive information in the memory, Secunia said.

"Unlike other browser flaws, this one is not subject to phishing or access to the system. But it can expose sensitive information from other Web sites you visited and the information you entered there," said Thomas Kristensen, Secunia chief technology officer.

While the flaw is only rated as "moderately critical" by Secunia, the rapid adoption of the open-source browser means that many users may be at risk. Prior to the release of version 1.0, downloads of earlier versions of the browser had reached 8 million within the first 18 months.

The Mozilla Foundation, which makes the Firefox browser, is working on a patch, and no cases have been reported, a representative for the group said.

[Secunia](#) [2] has developed a [test](#) [3] that allows people to see whether their system is affected by the vulnerability.

[Source](#) [4]

[Security](#)

---

**Source URL:** <http://www.tuxmachines.org/node/484>

## Links:

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] <http://secunia.com/advisories/14820/>

[3] [http://secunia.com/mozilla\\_products\\_arbitrary\\_memory\\_exposure\\_test/](http://secunia.com/mozilla_products_arbitrary_memory_exposure_test/)

[4] [http://news.com.com/Flaw+found+in+Firefox/2100-1029\\_3-5655861.html?tag=nefd.top](http://news.com.com/Flaw+found+in+Firefox/2100-1029_3-5655861.html?tag=nefd.top)