

# [NEWS] Mozilla Platform's Code Execution Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0118.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 03/24/05

To: list@securiteam.com

Date: 24 Mar 2005 18:14:24 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Mozilla Platform's Code Execution Vulnerabilities

---

## SUMMARY

"The mission of the <www.mozilla.org> Mozilla project is to preserve choice and innovation on the Internet."

Several vulnerabilities were identified in Mozilla Suite, Firefox and Thunderbird, which may be exploited by attackers to execute arbitrary commands or bypass certain security features.

## DETAILS

### Vulnerable Systems:

- \* Mozilla Firefox version 1.0.1 and prior
- \* Mozilla Suite version 1.7.5 and prior
- \* Mozilla Thunderbird version 1.0.1 and prior

### Immune Systems:

- \* Mozilla Firefox version 1.0.2
- \* Mozilla Suite version 1.7.6
- \* Mozilla Thunderbird version 1.0.2

## Securiteam: [NEWS] Mozilla Platform's Code Execution Vulnerabilities

The first vulnerability is due to a heap overrun error when processing a Netscape-specific extension block in GIF images, which may be exploited to run arbitrary code on a vulnerable system via a web page or email message containing a specially crafted GIF image.

The second flaw occurs if a user bookmarked a specially crafted page as a Firefox sidebar panel, which could be exploited to execute arbitrary programs by opening a privileged page and injecting JavaScript into it.

The third issue occurs when handling specially crafted XUL files, and may be exploited to bypass the restriction on opening privileged XUL.

### ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.k-otik.com/english/advisories/2005/0296>>  
<http://www.k-otik.com/english/advisories/2005/0296>  
<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=284627](https://bugzilla.mozilla.org/show_bug.cgi?id=284627)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=284627](https://bugzilla.mozilla.org/show_bug.cgi?id=284627)  
<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=285595](https://bugzilla.mozilla.org/show_bug.cgi?id=285595)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=285595](https://bugzilla.mozilla.org/show_bug.cgi?id=285595)  
<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=285438](https://bugzilla.mozilla.org/show_bug.cgi?id=285438)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=285438](https://bugzilla.mozilla.org/show_bug.cgi?id=285438)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.