

Securiteam: [NEWS] Flash Player Local Shared Object Vulnerability (Patch)

# [NEWS] Flash Player Local Shared Object Vulnerability (Patch)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0051.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 12/18/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 18 Dec 2003 10:32:16 +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>

-----

Flash Player Local Shared Object Vulnerability (Patch)

---

## SUMMARY

A recently discovered security flaw in the Internet Explorer and Opera browsers may allow improper access to certain local files. A potential exploit can then be created in association with the local Flash data file to allow a malicious user to gain access to information stored on the local machine.

## DETAILS

Solution:

Macromedia has released an updated version of Macromedia Flash Player (7,0,19,0) that can be downloaded from the Macromedia Player Download Center.

This new version stores local data in a way that a malicious user cannot access it from applications other than Flash Player. This ensures Flash movies are able to work properly with data saved to the local file system, but external applications, such as web browsers, are not.

Severity Rating:

Securiteam: [NEWS] Flash Player Local Shared Object Vulnerability (Patch)

Macromedia categorizes this issue as an important update and recommends users update to the newest player.

Technical Details:

This release of Flash Player addresses the potential for exploits due to the predictability of the location of data stored by the Flash movies. While this is not in itself a directly exploitable vulnerability, an exploit can be created in combination with a security flaw in the browser. If the data stored by Flash Player on the local file system is a script, then it may be possible for that script to be executed on the local machine using a browser.

This update prevents data stored by Flash movies from being used maliciously. However, at this time no updates to Internet Explorer and Opera browsers addressing the vulnerabilities in those products have been announced.

ADDITIONAL INFORMATION

The information has been provided by <mailto:secure@macromedia.com> Macromedia Security Center.

=====

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 In order to subscribe to the mailing list, simply forward this email to: 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.