

# [EXPL] Buffer Overrun in JPEG Processing Proof Of Concept (MS04-028)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0053.html>

---

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

**Date:** 09/21/04

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

Date: 21 Sep 2004 13:54:55 +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>

-----

Buffer Overrun in JPEG Processing Proof Of Concept (MS04-028)

---

## SUMMARY

In a previously featured article,

<<http://www.securiteam.com/windowsntfocus/5VP0H1FE0W.html>> Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028), a buffer overrun in the GDI+ library was reported. Provided below is a proof of concept example that will crash various applications attempting to open the malicious JPEG image.

## DETAILS

A proof of concept JPEG image that will crash an application attempting to open/preview it on an affected platform can be downloaded from

<<http://www.gulftech.org/?node=downloads>>

<http://www.gulftech.org/?node=downloads>

The vulnerability in the comment parsing of the JPEG file is similar to a previous vulnerability found almost two years ago regarding Netscape handling of JPEG images. A more thorough analysis of the code and methods of exploitation can be found at

<<http://www.openwall.com/advisories/OW-002-netscape-jpeg/>>

Securiteam: [EXPL] Buffer Overrun in JPEG Processing Proof Of Concept (MS04-028)

<http://www.openwall.com/advisories/OW-002-netscape-jpeg/> .

Some antivirus software can detect the presence of such a malicious JPEG image since the problem is specific in nature and a signature identification can be made. McAfee's antivirus with virus definitions version 4.0.4393 or greater can detect the problem.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@gulftech.org>  
GulfTech Security.

=====

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.