

# [VulnWatch] Abobe Reader 5.1 XFDF Buffer Overflow Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-03/0001.html>

---

**From:** NGSSoftware Insight Security Research (*nistr\_at\_nextgenss.com*)

**Date:** 03/04/04

To: <bugtraq@securityfocus.com>, <NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM>, <vulnwatch@vulnwatch.org>

Date: Wed, 3 Mar 2004 23:18:54 -0000

## NGSSoftware Insight Security Research Advisory

Name: Adobe Acrobat Reader XML Forms Data Format Buffer Overflow

Systems Affected: Adobe Acrobat Reader version 5.1

Severity: High Risk

Vendor URL: <http://www.adobe.com/>

Author: David Litchfield [ [david@ngssoftware.com](mailto:david@ngssoftware.com) ]

Date Vendor Notified: 7th February 2004

Date of Public Advisory: 3rd March 2004

Advisory number: #NISR03022004

Advisory URL: <http://www.ngssoftware.com/advisories/adobexfdf.txt>

## Description

\*\*\*\*\*

Adobe Acrobat Reader is a viewer that renders PDF documents. The Reader can be extended using the XML Forms Data Format or XFDF. XFDF is a format for representing forms data and annotations in a PDF document. XFDF files have a .xfdf extension and are rendered automatically on download when using applications such as Internet Explorer. Also note that, regardless of the file extension if the MIME type is set to "application/vnd.adobe.xfdf" the file will be treated as a XFDF. When parsing an XFDF document the Adobe Reader suffers from a classic stack based buffer overflow vulnerability.

## Details

\*\*\*\*\*

When the xfdf file is parsed an unsafe call to sprintf is made in preparation for outputting a debug message using OutputDebugString. Whether the process is being debugged or not the vulnerable code is still called. Rendering the file will trigger the overflow. A user would need to be enticed to a web site that hosted a malicious xfdf file or sent one via e-mail.

## Fix Information

\*\*\*\*\*

On contacting Adobe, they confirmed that the current version is no longer vulnerable and NGSSoftware urgently advises users of Adobe Reader to

## VulnWatch: [VulnWatch] Adobe Reader 5.1 XFDF Buffer Overflow Vulnerability

upgrade.

<http://www.adobe.com/support/downloads/main.html>

About NGSSoftware

\*\*\*\*\*

NGSSoftware design, research and develop intelligent, advanced application security assessment scanners. Based in the United Kingdom, NGSSoftware have offices in the South of London and the East Coast of Scotland. NGSSoftware's sister company NGSConsulting, offers best of breed security consulting services, specialising in application, host and network security assessments.

<http://www.ngssoftware.com/>

Telephone +44 208 401 0070

Fax +44 208 401 0076

[enquiries@ngssoftware.com](mailto:enquiries@ngssoftware.com)