

# [NT] Microsoft Publisher Font Parsing Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00013.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 13 Sep 2006 09:08:30 +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>

-----

Microsoft Publisher Font Parsing Vulnerability

---

## SUMMARY

Microsoft Publisher is a lightweight desktop publishing (DTP) application bundled with Microsoft Office Small Business and Professional. The application facilitates the design of professional business and marketing communications via familiar Office tools & functionality.

Unfortunately, it transpires that Microsoft Publisher is susceptible to a remote, arbitrary code execution vulnerability that yields full system access running in the context of a target user.

## DETAILS

Vulnerable Systems:

- \* Microsoft Publisher 2000 (Office 2000)
- \* Microsoft Publisher 2002 (Office 2002)
- \* Microsoft Publisher 2003 (Office 2003)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0001>>  
CVE-2006-0001

## [NT] Microsoft Publisher Font Parsing Vulnerability

The vulnerability emanates from Publishers inability to perform sufficient data validation when processing the contents of a .pub document. As a result, it is possible to modify a .pub file in such a way that when opened will corrupt critical system memory, allowing an attacker to execute code of his choice.

More specifically, the vulnerable condition is derived from an attacker controlled string that facilitates an "extended" memory overwrite using portions of the original .pub file.

As no checks are made on the length of the data being copied, the net result is that of a classic "stack overflow" condition, in which EIP control is gained via one of several return addresses.

### Exploitation:

As with most file orientated vulnerabilities, the aforementioned issue requires a certain degree of social engineering to achieve successful exploitation.

However, users of Microsoft Publisher 2000 (Office 2000) are at an increased risk due to the exploitability of the vulnerability in a possible web-based attack scenario.

### Disclosure timeline:

03/08/2005 – Preliminary Vendor notification.  
12/08/2005 – Vulnerability confirmed by Vendor.  
03/01/2006 – Public Disclosure deferred by Vendor.  
11/07/2006 – Public Disclosure deferred by Vendor.  
12/09/2006 – Coordinated public release.

Total Time to Fix: 1 year, 1 month, 6 days (402 days)

## ADDITIONAL INFORMATION

The information has been provided by Stuart Pearson.

The original article can be found at:

<<http://www.computerterrorism.com/research/ct12-09-2006-2.htm>>  
<http://www.computerterrorism.com/research/ct12-09-2006-2.htm>

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

[NT] Microsoft Publisher Font Parsing Vulnerability

=====  
=====

**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.