

# [NT] NJStar Word Processor Font Names Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00072.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 22 Feb 2006 16:23:57 +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>

-----

NJStar Word Processor Font Names Buffer Overflow

---

## SUMMARY

<<http://www.njstar.com/>> NJStar Word Processor "A Windows version word processor software, which is designed for both Chinese/Japanese and English languages."

Improper handling of font names in NJStar Word Processor allows attackers to execute arbitrary code.

## DETAILS

### Vulnerable Systems:

- \* NJStar Chinese/Japanese Word Processor 5.01.41108
- \* NJStar Chinese/Japanese Word Processor 4.x and 5.0x

### Immune Systems:

- \* NJStar Chinese/Japanese Word Processor 5.10

A vulnerability in NJStar Word Processor, can be exploited by malicious people to compromise a user's system.

## [NT] NJStar Word Processor Font Names Buffer Overflow

The vulnerability is caused due to a boundary error within the handling of font names read from a NJStar document file (".njs"). This can be exploited to cause a stack-based buffer overflow.

Successful exploitation allows arbitrary code execution when a malicious ".njs" file is opened.

### Disclosure Timeline:

03/02/2006 – Initial vendor notification.  
04/02/2006 – Initial vendor reply.  
18/02/2006 – Vendor released fixed versions.  
20/02/2006 – Public disclosure.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:remove-vuln@xxxxxxxxxxxxx>> Secunia Research.

The original article can be found at:

<[http://secunia.com/secunia\\_research/2006-5/advisory/](http://secunia.com/secunia_research/2006-5/advisory/)>  
[http://secunia.com/secunia\\_research/2006-5/advisory/](http://secunia.com/secunia_research/2006-5/advisory/)

=====

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@xxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxx)

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

=====

=====

### 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.