

# [NT] MailEnable POP Service "PASS" Command Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00029.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 19 Dec 2006 19:19:17 +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>

-----

MailEnable POP Service "PASS" Command Buffer Overflow

---

## SUMMARY

" <<http://mailenable.com/>> MailEnable's mail server software provides a powerful, scalable hosted messaging platform for Microsoft Windows. MailEnable offers stability, unsurpassed flexibility and an extensive feature set which allows you to provide cost-effective mail services". Secunia Research has discovered a vulnerability in MailEnable, which can be exploited by malicious people to compromise a vulnerable system.

## DETAILS

Vulnerable Systems:

- \* MailEnable Enterprise Edition version 2.35
- \* MailEnable Professional Edition version 2.35

The vulnerability is caused due to a boundary error in the POP service when handling arguments passed to the "PASS" command. This can be exploited to cause a stack-based buffer overflow by passing an overly long, specially crafted string as argument to the affected command.

Successful exploitation allows execution of arbitrary code.

[NT] MailEnable POP Service "PASS" Command Buffer Overflow

Solution:

Apply hotfix: <<http://www.mailenable.com/hotfix/ME-10026.EXE>>  
<http://www.mailenable.com/hotfix/ME-10026.EXE>

Time Table:

18/12/2006 – Vendor notified.  
18/12/2006 – Vendor response and hotfix released.  
18/12/2006 – Public disclosure.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6605>>  
CVE-2006-6605

ADDITIONAL INFORMATION

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

The original article can be found at:  
<[http://secunia.com/secunia\\_research/2006-75/](http://secunia.com/secunia_research/2006-75/)>  
[http://secunia.com/secunia\\_research/2006-75/](http://secunia.com/secunia_research/2006-75/)

=====

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

=====  
=====

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.