

[NT] Pegasus Mail Buffer Overflow and Off-by-One (POP3 reply, Email header)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00068.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 21 Dec 2005 17:00:28 +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>

Pegasus Mail Buffer Overflow and Off-by-One (POP3 reply, Email header)

SUMMARY

" <<http://www.pmail.com/>> Pegasus Mail is a free, standards-based electronic mail client suitable for use by single or multiple users on single computers or on local area networks."

A buffer overflow and a off by one vulnerabilities in Pegasus Mail allow remote attackers to cause the product to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Pegasus Mail version 4.21a, 4.21b, and 4.21c.
- * Pegasus Mail version 4.30PB1 (Public Beta 1).

Immune Systems:

- * Pegasus Mail version 4.31

Buffer Overflow:

A boundary error exists when using the reply from a POP3 server to construct trace messages that are displayed to the user if an error occurs

[NT] Pegasus Mail Buffer Overflow and Off-by-One (POP3 reply, Email header)

when downloading emails. This can be exploited to cause a stack-based buffer overflow via an overly long POP3 reply.

Successful exploitation allows arbitrary code execution but requires that the user is e.g. tricked into connecting to a malicious POP3 server.

Off by one:

An off-by-one error exists when displaying the <<http://www.faqs.org/rfcs/rfc2822.html>> RFC2822 message headers of an email to the user. This can be exploited to overwrite the least significant byte of the saved EBP via a email message header that is 1022 bytes or longer. This allows code execution on a Windows XP system.

Successful exploitation requires that the user is e.g. tricked into viewing the headers of a malicious email via the "Message headers..." menu item in the context menu of the email message.

Disclosure Timeline:

- 13/12/2005 – Initial vendor notification.
- 13/12/2005 – Initial vendor reply.
- 20/12/2005 – Public disclosure.

ADDITIONAL INFORMATION

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

The original article can be found at:
<<http://secunia.com/advisories/17992/>>
<http://secunia.com/advisories/17992/>

=====

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

=====
=====

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.

[NT] Pegasus Mail Buffer Overflow and Off-by-One (POP3 reply, Email header)

- Prev by Date: [*\[UNIX\] Blender Integer Overflow Vulnerability \(BlenLoader, get_bhead\)*](#)
- Next by Date: [*\[NEWS\] Google.com UTF-7 XSS Vulnerabilities*](#)
- Previous by thread: [*\[UNIX\] Blender Integer Overflow Vulnerability \(BlenLoader, get_bhead\)*](#)
- Next by thread: [*\[NEWS\] Google.com UTF-7 XSS Vulnerabilities*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)