

# [NT] Remote PGP Outlook Encryption Plug-in Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0036.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 07/11/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 11 Jul 2002 06:33:00 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> - Know that you're safe.

-----

Remote PGP Outlook Encryption Plug-in Vulnerability

---

## SUMMARY

A vulnerability in the NAI PGP Outlook plug-in can be exploited to remotely execute code on any system that uses the NAI PGP Outlook plug-in's. By sending a carefully crafted email, the message decoding functionality can be manipulated to overwrite various heap structures pertinent to the PGP plug-in.

This vulnerability can be exploited by a user simply selecting a "malicious" email the opening of attachments is not required. When the attack is performed against a target system, malicious code will be executed within the context of the user receiving the email. This can lead to the compromise of the targets machine, as well as their PGP encrypted communications. It should also be noted that because of the nature of the SMTP protocol this vulnerability could be exploited anonymously.

## DETAILS

Vulnerable systems:

- \* NAI PGP Desktop Security 7.0.4
- \* NAI PGP Personal Security 7.0.3
- \* NAI PGP Freeware 7.0.3

## Securiteam: [NT] Remote PGP Outlook Encryption Plug-in Vulnerability

### Exploitation:

By creating a malformed email, we can overwrite a section of heap memory that contains various data. By overwriting this section of heap with valid addresses of an unused section in the PEB, which is the same across all NT systems, we can walk the email parsing and eventually get to something easily exploitable:

```
CALL DWORD PTR [ecx]
```

This pointer addresses references a function pointer list. At the time of exploitation, an attacker controlled buffer address is the first item on the stack. By overwriting the function pointer list pointer address with the address of an Import table, we can call any imported function. Our current stack will be passed into the function for parameter use, as is. The first item on our stack is an address that points to attacker-controlled data.

By overwriting the address, with the address of the SetUnhandledExceptionFilter() IAT entry, execution will redirect into this address when the default exception handler is called,

After returning from SetUnhandledExceptionFilter() PGP Outlook will fail as it crawls back down the call stack, after cycling through the exception list it will call the DefaultExceptionHandler, which now contains the address of our code. This of course can also be exploited silently using frame reconstruction.

Due to the large size of an example vulnerable email, we are not including it in our advisory. We will be updating the research section of our website with a link to an example email.

### Vendor Status:

NAI has worked quickly to safeguard customers against this vulnerability. They have released a patch, for the latest versions of the PGP Outlook plug-in, to protect systems from this flaw. You may download the patch from:

<http://www.nai.com/naicommon/download/upgrade/patches/patch-pgphofix.asp>  
<http://www.nai.com/naicommon/download/upgrade/patches/patch-pgphofix.asp>

Note: This issue does not affect PGP Corporate Desktop users.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[marc@eeye.com](mailto:marc@eeye.com)> Marc Maiffret.

=====

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@securiteam.com](mailto:list-unsubscribe@securiteam.com)

Securiteam: [NT] Remote PGP Outlook Encryption Plug-in Vulnerability

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

=====  
=====

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.

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] IE Allows Universal Cross Domain Scripting"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)