

# [NT] PGP Desktop Medium Risk Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00003.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 1 Feb 2007 17:49:19 +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>

-----

PGP Desktop Medium Risk Vulnerability

---

## SUMMARY

Peter Winter-Smith of NGSSoftware has discovered a medium risk vulnerability in PGP Desktop which can allow a remote authenticated attacker to execute arbitrary code on a system on which PGP Desktop is installed.

## DETAILS

Vulnerable Systems:

- \* PGP Desktop version 9.5.0 and prior

Immune Systems:

- \* PGP Desktop version 9.5.1

The vulnerability resides within the Windows Service which PGP Desktop installs (which operates under the Local System account), and as such it may be used by any local or remote user (who must be a member of at least the Everyone/ANONYMOUS LOGON groups) to run code with escalated privileges. NGS have not been able to exploit this issue in the context of a NULL session.

## [NT] PGP Desktop Medium Risk Vulnerability

The details of this issue are as follows:

PGP Desktop installs a service (PGPServ.exe/PGPsdkserv.exe) which exposes a named pipe '\pipe\pgpserv' (or '\pipe\pgpsdkserv' for the PGPsdkserv.exe instance). This pipe is the endpoint for an RPC interface (uuid:15cd3850-28ca-11ce-a4e8-00aa006116cb) which takes the following format:

```
[ uuid(15cd3850-28ca-11ce-a4e8-00aa006116cb),
  version(1.0),
  implicit_handle(handle_t rpc_binding)
] interface pgpsdkserv
{
  error_status_t Function_00(
[in] /* [ignore] void */ long element_1
);

  typedef struct {
  long element_2;
  [size_is(element_2)] [unique] byte *element_3;
  } TYPE_1;

  error_status_t Function_01(
[in] /* [ignore] void */ long element_4,
[in] [size_is(element_6)] byte element_5[*],
[in] long element_6,
[in] long element_7,
[out] [ref] TYPE_1 *element_8
);
}
```

This interface is used to marshall various objects and information between PGP clients (PGP.dll/PGPsdks.dll) and the PGP service.

The vulnerability occurs as a result of the fact that the code responsible for processing the objects which are passed over the interface to the service does not perform any kind of validation on these objects, and instead trusts that object data is completely safe in the form that it is received (i.e., absolute pointers are trusted without validation).

NGS have discovered that if the following object is passed over the interface as the second parameter to function ordinal 1, an absolute pointer is trusted and executed – easily facilitating arbitrary code execution inside of the PGP service process:

```
/*
```

structure passed over rpc:

```
struct {
  DWORD **pprgMM; // set as absolute pointer to dwUnknown_1
  DWORD dwUnknown_1; // set as absolute pointer to 'rgMM'
  DWORD dwCount; // set to value 0
```

[NT] PGP Desktop Medium Risk Vulnerability

```
DWORD dwFGUB_signature; // set to value 'FGUB'  
DWORD dwUnknown_2; // set to value 'rgMM'  
DWORD dwUnknown_3;  
DWORD dwUnknown_4;  
DWORD dwUnknown_5;  
DWORD dwUnknown_6;  
PBYTE pbFunction; // set to absolute address of shellcode  
// etc...  
};  
  
*/
```

Vendor Status:

This issue has been resolved as of PGP Desktop 9.5.1 and NGS recommend that all users download the updated version from the PGP website:  
<<http://www.pgp.com/>> <http://www.pgp.com/>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@xxxxxxxxxxxxxxxx>>  
NGSSoftware Insight Security Research.

=====

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

=====  
=====

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.