

[NT] PGP Desktop Wipe Free Space Flaw

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00033.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 13 Dec 2005 17:46:29 +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 Wipe Free Space Flaw

SUMMARY

" <<http://www.pgp.com/products/desktop/index.html>> PGP Desktop Professional provides comprehensive security for individual desktops, making it possible for organizations to protect sensitive information for a single person without changing the existing IT infrastructure or disrupting work processes."

PGP Wipe does not clean the file's slacks on NTFS partition, allowing recovery of deleted data.

DETAILS

Vulnerable Systems:

- * PGP Desktop Professional version 9.0.3 Build 2932
- * PGP Desktop version 8.x (all versions tested were vulnerable)

PGP Desktop includes a Wipe Free Space utility that claims to eliminate data in all the free space on your hard drive including the the little areas after the end of existing files which may still have old data left behind. In short, the utility claims to wipe file slack space, the unused space in a disk cluster. The software does not work as advertised. It does

[NT] PGP Desktop Wipe Free Space Flaw

not clean slack space.

NTFS volumes allocate space for files based on fixed cluster sizes. By default, an NTFS drive will allocate 4096 bytes per cluster. Each cluster is sub-divided into 512 byte sectors, by default. Because of the allocation by cluster, a file 9024 bytes in size would require more than 4096 bytes, more than 8192 bytes, but less than 12288 bytes. The file system must allocate 12288 bytes to store the file.

File slack space is the unused series of bytes from the end of a file to the end of the disk cluster. For example lets have a gif file that is a 3264 bytes of slack space exists. When the file F:\AG00004_.GIF, is seen through Windows Explorer with a file size of 9k. When seen through EnCase, the file actually occupies 9024 bytes of the 12288 bytes allocated for it on disk. The series of red zeros in the lower left pane represents the file's slack space, currently empty.

After verifying that the slack space is empty, some tools can be used to store data within the slack space of the file. Below the slack space of the file is examined with the EnCase forensic software after Slacker is used to store data in the empty space.

According to PGP Professional, the slack space after the files should now have been cleaned of any data, but a forensic acquisition of the drive with both EnCase and WinHex after the Wipe Free Space utility has been run shows us that the data has not been changed at all.

Vendor Status:

PGP has been notified of this issue on multiple occasions, but has chosen not to respond.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sflist@xxxxxxxxxxxxxxxxxxxx>> H D Moore.

The original article can be found at:

<http://metasploit.com/research/vulns/pgp_slackspace/>
http://metasploit.com/research/vulns/pgp_slackspace/

=====

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.

- Prev by Date: [*\[TOOL\] MS SQL Server Captured Authentication Packets Cracker*](#)
- Next by Date: [*\[NT\] Lyris ListManager Multiple SQL Injection, information Disclosure and Authentication Bypassing*](#)
- Previous by thread: [*\[TOOL\] MS SQL Server Captured Authentication Packets Cracker*](#)
- Next by thread: [*\[NT\] Lyris ListManager Multiple SQL Injection, information Disclosure and Authentication Bypassing*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)