

[NT] PGPDisk Available to Any "Switched User" Under Windows XP

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0096.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/22/03

To: list@securiteam.com

Date: 22 Oct 2003 11:15:18 +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>

PGPDisk Available to Any "Switched User" Under Windows XP

SUMMARY

When a user mounts a PGPDisk and for whatever reason leaves his computer, the PGP disk stays "mounted".

If another user, with a local login right, uses the Windows XP "switch user" function, he have full access to the mounted PGP Disk. The data is then locally compromised.

Under Windows 2000 and Terminal server activated, it is possible that the data become then remotely compromised.

DETAILS

Mitigating factors:

* If you log off, the disk is automatically unmounted.

* NTFS access rights can be defined on the PGP Volume (with the known limitation, regarding powerful users that can take ownership of files) and the question regarding the usage of PGP Disk if the only security is NTFS...

Securiteam: [NT] PGPDisk Available to Any "Switched User" Under Windows XP

* You can activate the auto unmount option after a certain period. The problem is that if you have files open, you may loose your work.

Vendor response:

The vendor has been contacted and acknowledges this was a "known" problem. However, they were not able to tell Thierry if they plan to fix this issue or not.

ADDITIONAL INFORMATION

The information has been provided by <mailto:thierry.deleeuw@advalvas.be>
Thierry De Leeuw.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.