

Securiteam: [NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

[NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0109.html>

From: support@securiteam.com

Date: 01/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 23 Jan 2002 20:55:23 +0100 (CET)

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.

Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

SUMMARY

The NTFS file system has a facility to bind additional data to a file or directory, called an alternate data stream (see: <http://www.securiteam.com/windowsntfocus/3H5PQS0N5G.html>> NTFS Hidden Streams. The perfect hiding place?). The alternate data streams cannot be removed, unless the parent file or directory is destroyed. Unfortunately, most file wiping utilities only deal with the primary data stream and do not wipe the alternate data streams, thus leaving data intact.

DETAILS

Vulnerable systems:

It is important to note that every single software package tested failed to erase single or multiple data streams (Eraser 5.3 erased multiple data streams in, however missed alternate data streams when only one was present in a file). Based on this we find it unlikely that any other secure deletion programs implement alternate data stream wiping properly, all secure deletion programs for Windows should be treated as suspect until proven innocent. If you are using secure deletion software, please check immediately for files with alternate data streams, and after deleting them you are strongly advised to wipe all free space.

Securiteam: [NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

<<http://www.bcwipe.com/>> BCWipe version 1.x and 2.x from Jetico – Confirmed in testing and from vendor.

<<http://www.tolvanen.com/eraser/>> Eraser 5.3 – Confirmed in testing and from vendor.

<http://www.accessdata.com/main_deleted_data.htm> SecureClean v3 build-2.0 – Confirmed in testing and from vendor.

<<http://www.east-tec.com/eraser/index.htm>> East-Tec Eraser 2000 – Confirmed in testing.

PGP 6.x <<http://www.pgpi.org/>> freeware and <<http://www.pgp.org/>> commercial, 7.x, freeware and commercial – Confirmed in testing.

Numerous other packages are suspected to be vulnerable, it is strongly advised to use the workarounds listed below.

Who should read this advisory:

Anyone using file wiping utilities such as PGP Wipe (from NAI), BCWipe (from Jetico) or East-Tec Eraser (from East-Tec) on a Windows system with an NTFS file system, such as Windows NT, Windows 2000 or Windows XP especially with features such as thumbnail pictures in explorer. This advisory affects virtually every Windows file wiping utility, none of the tested programs were found to be problem-free.

Impact:

If data is stored in an alternate data stream attached to a file (such as the thumbnail of an image) or directory when this file or directory is wiped the information contained within the alternate data stream will be left intact on the hard drive. No warning is given to the user at all by Windows or the wiping programs. For example if you use windows file explorer (the default file browser in Windows) and have thumbnails of pictures enabled (the default setting) then the thumbnail of the thumbnail image, once created (i.e. once the directory is viewed in Explorer) will not be deleted until you delete the file and wipe all free space.

Alternate data streams also provide an ideal location to keep attack tools, snippets of virus code and so forth for attackers and viruses, in fact some virus scanners do not scan alternate data streams unless specifically configured to do so (often labeled as "scan all files" or similar).

The good news is that floppy disks and most other removable media are not formatted as NTFS, thus it is unlikely that copied files will contain the alternate data streams. As well no all compression programs, such as WinZip copy the alternate data streams, while others such as WinRAR do copy the alternate data streams. While it is unlikely that files with alternate data streams will have made it to other systems with their alternate data streams intact it is possible, and any systems that have had sensitive data copied or moved to them should immediately have their free space wiped in order to ensure alternate data streams containing sensitive information are still present.

Details:

Create a file with an alternate data stream:

Securiteam: [NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

```
echo "this is a text file" > C:\file.txt
echo "this is the alternate data stream lkajhk12" >
C:\file.txt:alternate-data-stream
```

If you use forensics software to examine the hard drive you will find the string of text "this is the alternate data stream lkajhk12" present on the drive. Now using the file wiper of your choice (BCWipe, etc.) choose the file C:\file.txt and wipe it. Use any many passes as you want. Now examine the drive for the string "this is the alternate data stream lkajhk12". You should be able to find it. To do this using Linux simply create an image file of the drive and examine it using grep or strings:

```
dd if=/dev/hdb1 of=windows-disk.img
grep "this is the alternate data stream lkajhk12" windows-disk.img
Or
strings windows-disk.img > windows-disk.strings grep "this is the
alternate data stream lkajhk12" windows-disk.strings
```

As you will quickly discover the data is easily found.

Alternate data streams are only available on NTFS file systems, making home users with older systems (Windows 95, Windows 98, and Windows ME) immune to this problem, but newer systems based on WindowsXP are capable of using NTFS, thus potentially exposing customers to risk. NTFS is also available on most corporate systems such as Windows NT, Windows 2000, and Windows XP. Another "feature" of alternate data streams is that they cannot be deleted. If you have an alternate data stream attached to a file, you cannot delete it, you can write other data to the stream, and however you cannot reliably delete it. To overwrite an alternate data stream simply place more data into it, for example:

```
echo "this will overwrite existing data in the stream" >
C:\file.txt:alternate-data-stream
Or
type notepad.exe > C:\file.txt:alternate-data-stream ***
```

Solutions and workarounds:

Several workarounds exist, and several vendors are in the process of updating software so as to fix the problem.

The first workaround is to avoid using alternate data streams to store sensitive information. Unless you have explicitly created alternate data streams, it is unlikely that they exist. However to check for alternate data streams several free tools exist, one of the best of which is <http://www.heysoft.de/nt/ep-lads.htm> LADS from Frank Hayne Software. Simply download lads.zip and unpack it, then run it from your root drives (e.g. C:\, D:\) and it should find and report all alternate data streams present. Because alternate data streams cannot be deleted tools to detect them are quite effective, once found you should securely delete the files and proceed to the next workaround, wiping free space, in order to ensure the alternate data streams are deleted.

Securiteam: [NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

The second workaround is to immediately use the "wipe free space" feature present in most secure file deletion utilities. Since the parent file or directory that the alternate data streams were attached to have been deleted the data in the alternate data streams is now in "free space" on the hard drive, thus using "wipe free space" will overwrite it. The downside of this workaround of course is that wiping all the free space on a hard disk can take quite some time, especially on a modern disk that may have several tens of gigabytes of free space to wipe. One note on this: wiping free space may not be possible or effective on network shares using NTFS, it is recommended to encrypt truly sensitive data on NTFS network file systems.

A third workaround is to encrypt sensitive data, Windows 2000 offers encrypted file system, or you can use programs such as PGP's <<http://www.pgp.com/products/desktop-privacy.asp>> PGPDisk or Jetico's <<http://www.jetico.com/index.htm#/products.htm>> BestCrypt. It is recommended to use encrypted disk partitions rather than encrypting single files, encrypted disk partitions are much easier to work with, type in a password and you have access, when you are done you do not need to worry about encrypting the file, as the data is kept in an encrypted state on the hard drive. Additionally temporary files stored in the same directory (such as opened word files) will also be kept in an encrypted state, reducing the need for you to wipe free space.

Vendors responses:

Several vendors have announced new versions in light of this, see below for more information:

BCWipe 1.x and 2.x

"We confirm importance of the problem of wiping alternate data stream in files, created on NTFS disks. We would thank Mr. Seifried for writing us about the problem and are going to solve it in the next version 3 of BCWipe, which is planned to be released at April, 2002."

SecureClean

"We will be covering all those issues in the next release. We plan to be shipping the product in February. The new release will be posted at www.accessdata.com. The current SecureClean does not handle alternate data streams or the thumbnails. That is coming in February."

East-Tec Eraser 2000

"EAST Technologies has acknowledged the possible problem concerning the wiping of the alternate data streams that may appear on NTFS disk drives and it will analyze this problem in the security product that it develops and the way this may compromise the user's personal security and privacy. EAST Technologies will also inform all its users and customers and in case it would be necessary, it will develop a fix."

Additional information:

Check your anti-virus software, several packages do not scan alternate data streams by default, it is recommended you enable scanning of all files and confirm by placing the

Securiteam: [NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS

<http://www.eicar.org/anti_virus_test_file.htm> eicar.com test file in an alternate data stream of a file and scanning to test. Backup programs should also be checked, attach an alternate data stream to a file, delete and then restore it, check for the alternate data stream. You can remove an alternate data stream either by copying the parent file onto non NTFS media or backing it up with a program that does not save the alternate data stream, or by using the "rm" utility present in MKS Software's "MKS Toolkit 8.0". An op-ed piece on this problem will be appearing at <<http://searchsecurity.com/>> SearchSecurity later this week.

References:

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/reskit/prkc_fil_xurt.asp>
Multiple data streams
<<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q286797>> Windows File Protection and Alternative Data Streams (Q286797)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:kurt@SEIFRIED.ORG>> Kurt Seifried.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Gaining Root Access via PHP.exe"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)