

# [NT] Windows VDM #UD Local Privilege Escalation

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0048.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 10/13/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Oct 2004 18:06:07 +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 VDM #UD Local Privilege Escalation

---

## SUMMARY

eEye Digital Security has discovered a third local privilege escalation vulnerability in the Windows kernel that would allow any code running on an affected system to elevate itself to the highest possible local privilege level (kernel), regardless of the privileges with which the code executes initially. For instance, a malicious user with legitimate access to a machine, or a remote attacker or worm payload able to gain unprivileged access through an unrelated exploit, could leverage this vulnerability to fully compromise a Windows NT 4.0, Windows 2000, Windows XP, or Windows Server 2003 system.

This vulnerability is located in a portion of the Windows kernel that handles some low-level aspects of executing 16-bit code inside a Virtual DOS Machine (VDM). A certain invalid opcode byte sequence is used in the 16-bit DOS emulation code to pass requests (referred to as "bops") to the 32-bit VDM "host" code, and the invalid opcode fault handler within the Windows kernel gives these sequences special treatment when relaying them to the 32-bit host code executing in user space (normally an NTVDM.EXE process). The kernel does not validate the address to which execution is transferred after one of these invalid instructions is encountered, and because the memory containing the address is fully accessible to user-mode code, it is possible to redirect execution to an arbitrary location with

## Securiteam: [NT] Windows VDM #UD Local Privilege Escalation

kernel privileges still in effect.

### DETAILS

The interrupt 06h (#UD) handler in NTOSKRNL.EXE contains a branch of code for quickly handling C4h/C4h machine code byte sequences according to the control word specified in the two bytes that follow, when the sequence occurs in Virtual-8086 mode (bit 17 of EFLAGS is set). If a control word value other than 4250h or 4350h (both used for fast file I/O) is given, the "bop" is passed off to another section of code in the process hosting the VDM. In NTVDM.EXE, this transition normally corresponds to returning from a call to NtVdmControl(0) (VdmpStartExecution), but in actuality, execution can be redirected anywhere, since the switch is just accomplished by swapping out context structures. The VDM TIB (arrived at by way of [[[[FFDFF124h]+44h]+1DCh]+98h] on Windows 2000, FS:[F18h] on Windows NT 4.0, Windows XP, and Windows Server 2003) is used to hold a copy of the V86-mode context in effect at the time the fault occurred (at offset +CD0h on NT4 and 2000, +2D8h for XP and 2003), then the context for resuming execution of the host code is retrieved (from offset +A04h on NT4 and 2000, +0Ch on XP and 2003) and loaded into the appropriate registers.

As mentioned above, this context is contained in user memory but is not sanitized in any way by the #UD handler, so any process with or without a formally-initialized VDM can place arbitrary values in the host execution context and get the handler to IRETD to any CS:EIP, allowing kernel privileges to be retained while user-supplied code is executed. On any version of Windows, it is sufficient to modify the VDM TIB in a process with a properly initialized VDM (most easily done by code executing in a COM file). For Windows NT 4.0, XP, and 2003, it is only necessary to set the pointer at offset F18h in the user-land TIB to reference a fake VDM TIB, then execute V86-mode code using NtContinue().

### Vendor Status:

Microsoft has released a patch for this vulnerability. The patch is available at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-032.msp>>  
<http://www.microsoft.com/technet/security/bulletin/MS04-032.msp>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:dsoeder@eeye.com> Derek Soeder.

The original article can be found at:

<<http://www.eeye.com/html/research/advisories/AD20041012.html>>  
<http://www.eeye.com/html/research/advisories/AD20041012.html>

=====

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

Securiteam: [NT] Windows VDM #UD Local Privilege Escalation

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.