



URGENT

LiveSecurity® Service



Update: 11 Windows Patches, 5 Rated Critical

MS10-015 COULD CAUSE BSOD ON XP MACHINES

SEVERITY: HIGH

11 February, 2010

UPDATE:

On 9 February, 2010, we alerted LiveSecurity subscribers about 11 Windows security bulletins that Microsoft released during their February Patch Day. The bulletins provided patches to fix over 19 security vulnerabilities affecting various components that ship with Windows. At the time, we recommended you download, test, and deploy those patches as quickly as possible.

Since our original alert, we have learned that one of Microsoft's patches may incapacitate Windows XP and cause a "[Blue Screen of Death](#)" (BSOD). After installing Microsoft's patches, many customers have reported that their XP computers would not completely boot, and instead would end up with a BSOD screen. Users experiencing this problem can not even boot Windows in "Safe Mode," completely preventing them from using their computers. At this time, the only known way to fix this problem is to boot using your Windows XP disc, start the Windows recovery console, and manually uninstall the recent Windows updates (you can find more info about this process [here](#)). While Microsoft hasn't officially reported which update causes this problem, many victims suspect Microsoft's [MS10-015](#) update as the culprit. So you may get away with just uninstalling that particular update (KB977165). You can learn more about these recent BSOD problems from [this ComputerWorld article](#).

So what's our advice? If you have already installed Microsoft's update and haven't experienced this problem, you can probably rest easy. However, if you haven't yet installed Microsoft's updates, we *highly* recommend you first **test** the patches on a non-production machine before deploying them throughout your network. In fact, this is the advice we *always* give when dealing with Microsoft updates; download, **test**, and only then deploy. While Microsoft has gotten much better at releasing stable updates over the years, past negative experiences with Microsoft updates have made many IT folks leery of them. This is why we suggest you always test their patches before deploying them. Finally, you may also consider holding off on applying the [MS10-015](#) patch until Microsoft responds to this issue. The kernel vulnerabilities that that particular update fixes primarily pose an internal risk, so they're not as severe as some of the other security vulnerabilities fixed on Tuesday. You can probably afford to wait until Microsoft updates that patch (assuming it really is the culprit for this issue).

If and when Microsoft officially responds to these incidents, and releases any updates, we will let you know.

For additional details about the vulnerability, and as a convenient reference, we reproduce our original 9 February alert below. You can also find it in the LiveSecurity [Latest Broadcasts](#) archive. (The web version of the 11 February alert will be available soon).

SUMMARY:

- **These vulnerabilities affect:** All current versions of Windows and components that ship with it
- **How an attacker exploits them:** Multiple vectors of attack, including sending specially crafted network packets, or enticing your users to open malicious media
- **Impact:** Various results; in the worst case, an attacker can gain

complete control of your Windows computer

- **What to do:** Install the appropriate Microsoft patches immediately, or let Windows Automatic Update do it for you.

EXPOSURE:

Today, Microsoft released eleven security bulletins describing over 19 vulnerabilities that affect Windows and components that ship with it. Each vulnerability affects different versions of Windows to varying degrees. However, a remote attacker could exploit the worst of these flaws to gain complete control of your Windows PC. The summary below lists the vulnerabilities, in order from highest to lowest severity.

- **MS10-006: SMB Client Code Execution Vulnerabilities**

Microsoft [Server Message Block \(SMB\)](#) is the protocol Windows uses for file and print sharing. According to Microsoft, the Windows SMB client suffers from two code execution vulnerabilities. Though the flaws differ technically, an attacker could exploit both in the same way. By enticing one of your users to connect to a malicious SMB server, an attacker can exploit either flaw to gain complete control of a vulnerable Windows computer.

Microsoft rating: **Critical.**

- **MS10-007: Shell Handler Code Execution Vulnerability**

Windows ships with the Windows [Shell application programming interface \(API\)](#), which allows other programs to perform certain Shell operations (such as execute a program). Unfortunately, one of the Shell API's functions (ShellExecute) doesn't properly validate data. Attackers can leverage this flaw to execute code. More specifically, by enticing one of your users to a specially crafted web page, an attacker can force Windows to invoke this insecure API function and execute arbitrary code on that user's computer. If your user has administrative privileges, the attacker would gain complete control of that user's PC.

Microsoft rating: **Critical.**

- **MS10-008: Cumulative ActiveX Kill Bit Update**

Microsoft and external researchers have identified several Microsoft and third party ActiveX controls that suffer various security vulnerabilities. By enticing one of your users to a malicious website, an attacker could exploit any of these ActiveX controls to execute code on your user's computer, with that user's privileges. Like most Windows vulnerabilities, if your user has administrative privileges, the attacker would gain complete control of the user's PC. This update sets the Kill Bit for all the vulnerable ActiveX controls, thereby disabling them in Windows.

Microsoft rating: **Critical.**

- **MS10-009: Multiple Windows TCP/IP Stack Vulnerabilities**

The TCP/IP stack that ships with Windows Vista and Server 2008 suffers from three code execution vulnerabilities and a [Denial of Service \(DoS\)](#) vulnerability. In all cases, an attacker exploits these flaws by sending specially crafted TCP/IP packets to your Windows computers. The three code execution flaws obviously pose the greatest threat. However, mitigating circumstances significantly lessen their real-world risk. For instance, two of the flaws require you use IPv6 networking (which few do) and the third only affects users that have installed a custom network driver. That said, if an attacker can exploit any of these three vulnerabilities, he will gain complete control of your Windows machines. On the other hand, attackers can easily exploit the fourth vulnerability, simply by sending a few specially crafted packets. However, the attacker could only exploit this flaw to crash or reboot your Windows computer.

Microsoft rating: **Critical.**

- **MS10-013: DirectShow Heap Buffer Overflow Vulnerability**

DirectShow is one of the DirectX components Windows uses to display graphics and media. DirectShow suffers from a heap [buffer overflow vulnerability](#) involving its inability to handle specially malformed AVI video files. By enticing one of your users to download and view a malicious video, or to visit a website with an embedded video, an attacker can exploit this flaw to execute code on that user's computer, with that user's privileges. If your user has administrative privileges, the attacker gains complete control of that user's PC.

Microsoft rating: **Critical.**

- **MS10-010: Windows Server 2008 x64 Hyper-V DoS Vulnerability**

Hyper-V is the hypervisor-based technology that provides a virtualization platform for Windows Server 2008 and Server 2008 R2. Unfortunately, Hyper-V suffers from a DoS vulnerability involving the way it parses specially encoded

machine instructions inside a guest virtual machine. By running a special program within a guest virtual machine, an attacker could exploit this flaw to lockup Hyper-V, causing all virtual machines to become non-responsive. However, in order to exploit this flaw, the attacker would first have to gain access to a guest virtual machine. This flaw only affects the x64 versions of Windows Server 2008.

Microsoft rating: **Important**.

- **MS10-011: CSRSS Local Elevation of Privilege Vulnerability**

The Client/Server Run-time SubSystem (CSRSS) is an essential Windows component responsible for console windows and creating and deleting [threads](#). It does not properly terminate user processes when users log out. By running a specially crafted program, an attacker could leverage this flaw to [elevate privileges](#), gaining complete control of a Windows computer. However, the attacker would first need to gain local access to a Windows computer using valid credentials (Guest access would work) in order to exploit this flaw.

Microsoft rating: **Critical**.

- **MS10-012: Various SMB Server Vulnerabilities**

As mentioned earlier, the [Server Message Block \(SMB\)](#) is the protocol Windows uses for file and print sharing. By default, Windows computers run the SMB Server service. Unfortunately, the SMB Server service suffers from four vulnerabilities: a Code Execution flaw, two DoS vulnerabilities, and an elevation of privileges vulnerability. Attackers could exploit all four flaws the same way - by sending specially crafted SMB packets to a vulnerable PC. However, the scope of each flaw differs significantly. For instance, the Code Execution vulnerability sounds bad, but an attacker can only exploit it if he first authenticates using valid user credentials. The two DoS vulnerabilities only allow an attacker to lockup the vulnerable system. Finally, an attacker could only exploit the elevation of privilege flaw to access an SMB share without authenticating; he couldn't exploit it to execute code.

Microsoft rating: **Important**.

- **MS10-014: Kerberos DoS Vulnerabilities**

[Kerberos](#) is one of the authentication protocols the server versions of Windows use. It suffers from a DoS vulnerability having to do with its inability to handle specially crafted ticket renewal requests. By sending a malicious ticket renewal request, an already authenticated attacker could exploit this flaw to lockup the vulnerable Windows server. However, the need for valid kerberos credentials significantly mitigates the risk of this flaw.

Microsoft rating: **Important**.

- **MS10-015: Windows Kernel Elevation of Privilege Vulnerabilities**

The [kernel](#) is core component of any computer operating system. The Windows kernel suffers from two elevation of privilege vulnerabilities. By running a specially crafted program, an attacker could leverage either of these flaws to gain complete control of your Windows computers. However, the attacker would first need to gain local access to your Windows computers using valid credentials. This factor significantly reduces the risk of these flaws.

Microsoft rating: **Important**

- **MS10-005: Microsoft Paint Integer Overflow Vulnerability**

Microsoft Paint is a basic painting application that ships with Windows. It suffers from an [integer overflow vulnerability](#) due to a flaw in the way it decodes [JPEG](#) images. If an attacker can convince one of your users to view a malicious JPEG image, specifically using the MS Paint program, the flaw can be exploited to execute code on that user's computer, with that user's privileges. Of course, if your user has local administrative privileges, the attacker gains total control of their computer.

Microsoft rating: **Moderate**.

SOLUTION PATH:

Microsoft has released patches for Windows which correct all of these vulnerabilities. You should download, test, and deploy the appropriate patches throughout your network immediately. If you choose, you can also let Windows Update automatically download and install these for you.

MS10-006:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)

- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)
- [Windows Vista](#)
- [Windows Vista x64](#)
- [Windows Server 2008](#)
- [Windows Server 2008 x64](#)
- [Windows Server 2008 Itanium](#)
- [Windows 7](#)
- [Windows 7 x64](#)
- [Windows Server 2008 R2 x64](#)
- [Windows Server 2008 R2 Itanium](#)

MS10-007:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)
- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)

Note: These vulnerabilities do not affect any other versions of Windows

MS10-008:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)
- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)
- [Windows Vista](#)
- [Windows Vista x64](#)
- [Windows Server 2008](#)
- [Windows Server 2008 x64](#)
- [Windows Server 2008 Itanium](#)
- [Windows 7](#)
- [Windows 7 x64](#)
- [Windows Server 2008 R2 x64](#)
- [Windows Server 2008 R2 Itanium](#)

MS10-009:

- [Windows Vista](#)
- [Windows Vista x64](#)
- [Windows Server 2008](#)
- [Windows Server 2008 x64](#)
- [Windows Server 2008 Itanium](#)

MS10-013:

- Windows 2000
 - [AVI Filter](#)
 - [Quartz](#)
 - [Quartz in DirectX 9.0](#)
- Windows XP

- [AVI Filter](#)
- [Quartz](#)
- Windows XP x64
 - [AVI Filter](#)
 - [Quartz](#)
- Windows Server 2003
 - [AVI Filter](#)
 - [Quartz](#)
- Windows Server 2003 x64
 - [AVI Filter](#)
 - [Quartz](#)
- Windows Server 2003 Itanium
 - [AVI Filter](#)
 - [Quartz](#)
- Windows Vista
 - [Quartz](#)
- Windows Vista x64
 - [Quartz](#)
- Windows Server 2008
 - [Quartz](#)
- Windows Server 2008 x64
 - [Quartz](#)
- Windows Server 2008 Itanium
 - [Quartz](#)
- Windows 7
 - [Quartz](#)
- Windows 7 x64
 - [Quartz](#)
- Windows Server 2008 R2 x64
 - [Quartz](#)
- Windows Server 2008 R2 Itanium
 - [Quartz](#)

MS10-010:

- [Windows Server 2008 x64](#)
- [Windows Server 2008 R2 x64](#)

MS10-011:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)
- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)

MS10-012:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)
- [Windows Server 2003](#)

- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)
- [Windows Vista](#)
- [Windows Vista x64](#)
- [Windows Server 2008](#)
- [Windows Server 2008 x64](#)
- [Windows Server 2008 Itanium](#)
- [Windows 7](#)
- [Windows 7 x64](#)
- [Windows Server 2008 R2 x64](#)
- [Windows Server 2008 R2 Itanium](#)

MS10-014:

- [Windows Server 2000](#)
- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)
- [Windows Server 2008](#)
- [Windows Server 2008 x64](#)

MS10-015:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)
- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)
- [Windows Vista](#)
- [Windows Vista x64](#)
- [Windows Server 2008](#)
- [Windows Server 2008 x64](#)
- [Windows Server 2008 Itanium](#)
- [Windows 7](#)

MS10-005:

- [Windows 2000](#)
- [Windows XP](#)
- [Windows XP x64](#)
- [Windows Server 2003](#)
- [Windows Server 2003 x64](#)
- [Windows Server 2003 Itanium](#)

FOR ALL WATCHGUARD USERS:

Attackers can exploit these flaws using diverse exploitation methods. A properly configured firewall can mitigate the risk of some of these issues. In fact, by default your Firebox will prevent most of the Microsoft flaws that require network access - specifically, the SMB-related vulnerabilities. You can also configure your Firebox to block the files types necessary to carry out some of these attacks.

That said, the Firebox cannot protect you from local attacks, nor can it prevent attacks that leverage normal looking HTTP traffic. Therefore, installing Microsoft's updates is your most secure course of action.

STATUS:

Microsoft has released patches correcting these issues.

REFERENCES:

- Microsoft Security Bulletin [MS10-005](#)
- Microsoft Security Bulletin [MS10-006](#)
- Microsoft Security Bulletin [MS10-007](#)
- Microsoft Security Bulletin [MS10-008](#)
- Microsoft Security Bulletin [MS10-009](#)
- Microsoft Security Bulletin [MS10-010](#)
- Microsoft Security Bulletin [MS10-011](#)
- Microsoft Security Bulletin [MS10-012](#)
- Microsoft Security Bulletin [MS10-013](#)
- Microsoft Security Bulletin [MS10-014](#)
- Microsoft Security Bulletin [MS10-015](#)

This alert was researched and written by Corey Nachreiner, CISSP.

What did you think of this alert? Let us know at your.opinion.matters@watchguard.com.

More alerts and articles: Log into the [LiveSecurity Archive](#).

NOTE:

This e-mail was sent from an unattended mailbox. Please do not reply.

ABOUT Questiva/TailoredMail:

WatchGuard has contracted with Questiva/TailoredMail, an industry leading vendor of trusted email services, to send these emails and maintain a record of your preferences confidentially. Personal information about you is not sold or rented to Questiva/TailoredMail or to other companies. Both WatchGuard and Questiva/TailoredMail are fully committed to your privacy, as detailed in WatchGuard's [privacy policy](#).

TO UNSUBSCRIBE: You received this e-mail because you subscribed to the WatchGuard LiveSecurity Service, which advises about virus alerts, security best practices, new hacking exploits, and more. If you no longer wish to be advised of these things, please let us know.

To unsubscribe on our web site, use our handy [web form](#).

To unsubscribe by postal mail, write to LiveSecurity Unsubscribe, 505 5th Avenue South, Suite 500, Seattle, WA 98104 - USA.

This email was sent to: jbecker@accessoe.com

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

Copyright 2009 WatchGuard Technologies, Incorporated. All Rights Reserved. WatchGuard, LiveSecurity and Firebox, and any other word listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein, are registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. *You may not modify, reproduce, republish, post, transmit, or distribute this content except as expressly permitted in writing by WatchGuard Technologies, Inc.*

Copyright © 1996 - 2009 WatchGuard Technologies, Inc.
All rights reserved. | [Terms of Use](#)

Postal Unsubscribe: LiveSecurity Unsubscribe, 505 Fifth Avenue South, Suite 500, Seattle, WA 98104