



## Update 2: 11 Windows Patches, 5 Rated Critical

### MS10-015 BSOD ONLY AFFECTS ROOTKIT INFECTED MACHINES.

**SEVERITY: HIGH**

18 February, 2010

#### UPDATE 2:

Last Thursday, we updated a Windows Information Alert, warning that one of Microsoft's patches ([MS10-015](#)) could cause a "Blue Screen of Death" (BSOD) on Windows XP computers. Some Windows users claimed their computer would not completely boot after applying Microsoft's new Windows kernel patch. Instead, the computer would stop at a BSOD screen. At the time, Microsoft had acknowledged the issue but had not completed their research on it, nor released an official response about it. Since then, Microsoft has [conclusively verified](#) that this BSOD issue only affects Windows computers that are infected with the [Alureon rootkit](#). If you apply the MS10-015 update while infected with the Alureon rootkit, your computer will get caught in the BSOD loop. You can learn much more about this issue in this [Microsoft Security Response Center blog post](#).

Now that Microsoft knows malware is responsible for this issue, they have no plans to update their patch. If you have already installed the MS10-015 update, you're good to go. If you have been holding off on the MS10-015 update, you can install it safely, assuming you are not infected with the Alureon rootkit. Microsoft [plans to release a tool](#) that will help you detect this rootkit in the future, but for now we recommend you do a full AV scan before installing MS10-015. You can also try F-Secure's free [Blacklight](#) rootkit scanner.

For additional details about the vulnerability, and as a convenient reference, we reproduce our original alert and update below.

---

#### 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.