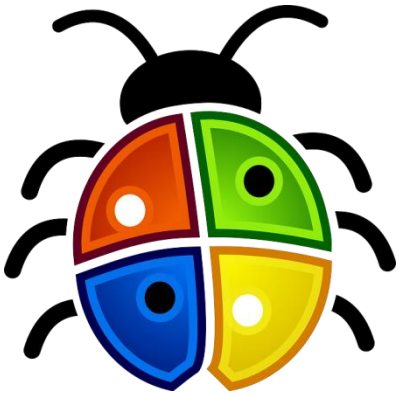
# Blog for MPA Networks

***https://www.mpa.com/blog.aspx?p=the-redirect-to-smb-bug-new-windows-same-danger***

# The ‘Redirect to SMB’ Bug: New Windows, Same Danger

Posted October 6, 2015



The big news out of Microsoft over the past couple of months is the much-ballyhooed release of Windows 10. While “Win10” finally addresses those annoying shortcomings of its predecessor Windows 8 (as we've discussed), it still hasn't corrected a dangerous security flaw known in cybersecurity circles as **Redirect to SMB**—a hidden vulnerability which has plagued all versions of Windows *since 1997.*

The original basis of Redirect to SMB was frighteningly simple: A victim simply needed to be duped into clicking on a URL (in a phony website or malicious email) that began with **file://** rather than the usual **http://** (e.g., file://12.34.567.89 or file://example.com). This would cause the victim's computer to directly link to the attacker's server via Server Message Block protocol (SMB), which would render the victim's computer under the attacker's control, and ultimately allow access to the victim's entire login credentials—usernames and passwords—for every protected business or personal account on the Internet.

## Redirect to SMB 2.0: Self-Service Cyber-Attacks

This past April, cybersecurity firm Cylance revealed they'd uncovered a potentially devastating new dimension to Redirect to SMB—which requires no additional trigger action on the part of the victim. Windows regularly issues automated "pings" via HTTP/HTTPS authentication for availability of updates and other routine background tasks.

Cylance discovered that these pings could be redirected from the legitimate HTTP destination to a rogue SMB server, enabling the attacker to swipe those valuable user logins. These threats aren't limited to the Windows operating system itself. After extensive testing, Cylance found exploitable Redirect to SMB vulnerabilities in over 30 "self-updating" Windows-based software products, including common applications you've probably used this week:

- Adobe Reader
- Apple Software Update (installs QuickTime and iTunes updates)
- Microsoft apps including Internet Explorer, Windows Media Player, and Excel 2010
- Antivirus programs from leading vendors including Norton, AVG, and Bitdefender

## "It Can't Happen To Me"—Until It Does!

Microsoft announced plans to deliver a security patch for Redirect to SMB way back in 2007, but has since publicly downplayed the likelihood of such attacks. (Of course, we remember how the Empire downplayed the likelihood of a direct hit to a small exhaust port destroying the Death Star!) We've talked at length about the legions of hackers around the world who've dedicated themselves to hijacking *your* computer. They read the same news reports we do, and we'd be surprised if some form of Redirect to SMB isn't on a crook or two's agenda.

In the meantime, **the most effective "workaround" against Redirect to SMB is to manually reconfigure a couple specific TCP ports in your firewall to restrict all outgoing SMB communication.** You'll block most external SMB-based attacks, but other useful Windows features may be affected. The release of Windows 10 was a welcome event, but remember that it's still not perfect. Rejoice over the return of the "Start" button—but keep security in mind. If you need help protecting your company against threats, get in touch today.