

Forum:[Hack Forums](#)

Thread: [Microsoft patches massive bug that allowed attackers to take complete control of PC's](#)

ZuGgY - February 11, 2015, 11:30 am

Quote:Today, Microsoft has issued a critical patch to every supported version of Windows that resolves a bug that may have been open for as long as fifteen years could allow attackers to remotely take control of Windows devices that connect to an Active Directory domain. The flaw — named 'Jasbug' — could allow someone to hijack a machine in a fairly straightforward manner. Microsoft said on its blog today it could be executed as follows: This is an example of a 'coffee shop' attack scenario, where an attacker would attempt to make changes to a shared network switch in a public place and can direct the client traffic an attacker-controlled system. In this scenario, the attacker has observed traffic across the switch and found that a specific machine is attempting to download a file located at the UNC path: \\10.0.0.100\Share\Login.bat . On the attacker machine, a share is set up that exactly matches the UNC path of the file requested by the victim: *\Share\Login.bat. The attacker will have crafted the contents of Login.bat to execute arbitrary, malicious code on the target system. Depending on the service requesting Login.bat, this could be executed as the local user or as the SYSTEM account on the victim's machine. The attacker then modifies the ARP table in the local switch to ensure that traffic intended for the target server 10.0.0.100 is now routed through to the attacker's machine. When the victim's machine next requests the file, the attacker's machine will return the malicious version of Login.bat. Uncovered by JAS Advisors and simMachines, it was reported in January 2014 and took over a year to resolve because it was a core Windows design problem, not a implementation problem. The researchers who found the bug said that "all computers and devices that are members of a corporate Active Directory network may be at risk." If successfully executed, attackers could take full control of a machine, install applications or create new user accounts. Microsoft's patch is available for download today from Windows Update, but it's not quite as easy as just installing the update this time around. The company is directing network administrators to this page for information on how to protect their domains against the attack. What's most alarming is despite Microsoft still supporting Windows Server 2003 for a further five months, the company will not be issuing a fix for this problem because "the architecture to support the fix [...] does not exist on Windows Server 2003." If you're still using a Windows Server 2003 domain, it's time to seriously consider upgrading. Home users don't appear to be directly at risk with this vulnerability, as domains are primarily used in businesses, but it's still worth installing the patch as soon as possible.

[Source](#)

Go do your updates ASAP, Windows users!

-Hyperion - February 11, 2015, 8:23 pm

Unless you use domains this threat is very low. But you should still always update windows