# غیر فعال کردن پروتکل SMBv1

بدافزارهای WannaCry و Petya از طریق یکی از حفرههای امنیتی ویندوز، منتشر شدند. پروتکل SMBv1 که بهصورت پیشفرض در سیستم عاملهای ویندوز فعال است، همان حفره امنیتی است. بنابراین اگر شما نیز از کاربران سیستم عاملهای ویندوز ۲، ۸ یا ۱۰ هستید، مطمئن شوید که این پروتکل بر روی سیستم عامل شما غیر فعال باشد.

#### SMBv1 چیست و چرا به صورت پیش فرض فعال است؟

SMBv1 یک پروتکل قدیمی است که ویندوز از آن برای اشتراک گذاشتن فایلها در یک شبکه محلی استفاده میکند. امروزه این پروتکل با نسخههای جدیدتر SMBv1 و SMBv2 و SMBv3 جدیدتر SMBv2 و SMBv3 و SMBv3

حال ممکن است این پرسش برایتان پیش بیاید که با وجود نسخههای جدید، دیگر چه نیازی به استفاده از نسخه قدیمی این پروتکل وجود دارد؟! در واقع، دلیل استفاده و فعال بودن این پروتکل بهصورت پیشفرض در سیستم عامل ویندوز این است که برخی برنامههای قدیمی همچنان با این نسخه کار میکنند و به نسخههای SMBv2 و SMBv3 آپدیت نشدهاند. لیست برنامههایی که همچنان به SMBv1 نیاز دارند را میتوانید در اینجا مشاهده نمایید.

اگر از هیچیک از نرمافزارهای این لیست استفاده نمی کنید، که احتمالا همینطور هم است، پیشنهاد می کنیم که هر چه سریعتر پروتکل SMBv1 را غیرفعال کنید تا سیستم خود را از هر گونه حمله احتمالی توسط بدافزارهای اشاره شده، محفوظ نگاه دارید. حتی کمپانی مایکروسافت نیز به کاربران پیشنهاد کرده است که در صورت عدم نیاز، این پروتکل را غیرفعال نمایند.

#### غیرفعال کردن SMBv1 را در ویندوز ۸ و ۱۰

مایکروسافت در بروزرسانی بعدی که در پاییز برای ویندوز ۱۰ ارائه خواهد کرد، پروتکل SMBv1 را بهصورت پیشفرض غیرفعال میکند. ولی تا آن زمان برای در امان ماندن از بدافزارها چه باید کرد؟

غیرفعال کردن SMBv1 در ویندوز ۸ و ۱۰ بسیار ساده است. به قسمت Control Panel بروید و بر روی گزینه SMBv1 در ویندوز ۸ و ۱۰ بسیار ساده است. به قسمت Control Panel بروید و بر روی گزینه SMBv1 در ویندوز ۸ و ۱۰ بسیار ساده است.

Control Panel\Programs						×
← → ~ ↑ 🖬 > Contro	ol Panel > Pro	ograms 🗸 🗸	5	Search Contr	rol Panel	Q
Control Panel Home System and Security Network and Internet Hardware and Sound	No.	Programs and Features Uninstall a program Turn Wi View installed updates Run programs made for previous v How to install a program	indow ersior	vs features on o	r off	
Programs User Accounts		Default Programs Change default settings for media Make a file type always open in a s	or dev pecifi	vices c program		

در پنجرهای که باز میشود، یه پایین صفحه بروید و گزینه SMB 1.0/CIFS Files Sharing Support را بیابید. تیک مربوط به این گزینه را بردارید تا پروتکل SMBv1 غیرفعال شود. سپس بر روی OK کلیک کنید.

0	Control Panel	🐻 Windows Features - 🗆 🔿	×	- 0	×
÷	⇒ ~ ↑ <b>(</b>	Turn Windows features on or off	9	Control Panel	Q
	Control Panel H	To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.		on or off	
	System and Secu	RIP Listener	^	en or en	
	Network and Int	Simple Network Management Protocol (SNMP)		ows	
	Hardware and S	Simple TCPIP services (i.e. echo, daytime etc)			
•	Programs	SMB 1.0/CIFS File Sharing Support			
	User Accounts	Support for the SMB 1.0/CIFS file sharing protocol, and the Comp	uter	1	
	Appearance and	Browser protocol.	_	1	
	Personalization	🗉 🗹 🔤 Windows PowerShell 2.0			
	Clock, Language	Windows Process Activation Service			
	Ease of Access	Windows Subsystem for Linux (Beta)			
		Windows TIFF IFilter			
		Work Folders Client	~		
		OK Cancel			

می ایست یک بار سیستم خود را Restart کنید تا تغییری که داده اید، اعمال شود.

## غیرفعال کردن SMBv1 در ویندوز ۷

روند غیرفعال کردن این پروتکل در ویندوز ۷ با ویندوز ۸ و ۱۰ تفاوت دارد. در ویندوز ۷ میبایست از طریق تغییر در رجیستری، این کار را انجام دهید.

قبل از اعمال هر گونه تغییری در رجیستری ویندوز، به یاد داشته باشید که ابزار ویرایش رجیستری یک ابزار بسیار قدرتمند است که میتواند در عین حال بسیار خطرناک باشد. چرا که اگر تغییرات و تنظیمات نادرستی در این محیط انجام دهید، ممکن است باعث اختلال در عملکرد سیستم عامل شود. بنابراین در هنگام کار با رجیستری، بسیار دقت کنید تا مشکلی برای سیستم شما پیش نیاید.

برای شروع، بر روی منوی Start کلیک کرده و عبارت regedit را تایپ کنید. بر روی آیکون رجیستری کلیک نمایید تا محیط ویرایش رجیستری باز شود.



در پنجره سمت چپ، مسیر زیر را دنبال کنید:

### $HKEY\_LOCAL\_MACHINE \SYSTEM \ Current Control Set \Services \Lanman Server \Parameters$

حال باید یک مقدار جدید در قسمت Parameters ایجاد کنید. برای این منظور روی گزینه Parameters کلیک راست کرده و گزینه New و پس از آن DWORD (32-bit) Valueرا انتخاب نمایید.

Regist	ry Editor						
File Edi	t View	Favorites	Help				
a 🤳 Lai	nmanServ	ver 🔺	Name		Туре	Data	
Aliases AutotunedParam DefaultSecurity Linkage Parameters Share Expand		(Default) AdjustedNullSes autodisconnect EnableAuthentic allog		REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD	(value not set) 0x00000003 (3) 0x00000000f (15) 0x00000001 (1)		
					0x00000	001 (1)	
D -	Share	New	•		Кеу		0 (0) 3 2d 6a 11 45 b4 44 b2 5f 78
Fir	Find		String Value			0 (0)	
👂 - 📗 lite	dio	Delete			Binary Value		
٠ <u>ااا</u>		Rename			DWORD (32-bit) Value D QWORD (64-bit) Value		
Computer	Computer\HKEY Export						arameters

نام این مقدار را SMB1 بگذارید.

DWORD مورد نظر ساخته میشود و مقدار پیشفرض آن ۰ خواهد بود. عدد ۰ نشان دهنده این است که SMBv1 غیر فعال است. بنابراین نیازی به تغییر مقدار DWORD نیست.

File Edit View Favorites	Help			
A 🌙 LanmanServer	Name	Туре	Data	
- Aliases	88 Guid	REG_BINARY	b6 89 bc e3 2d 6a 11 45 b4 44 b2 5f 78	
AutotunedParam	88 Lmannounce	REG_DWORD	0x00000000 (0)	
DefaultSecurity	ab NullSessionPipes	REG_MULTI_SZ		
	🔀 requiresecuritysi	REG_DWORD	0x00000000 (0)	
ShareProvider	nestrictnullsessa	REG_DWORD	0x00000001 (1)	
Shares	ab ServiceDII	REG_EXPAND_SZ	%SystemRoot%\system32\srvsvc.dll	
LanmanWorkstation	BerviceDIIUnloa	REG_DWORD	0x00000001 (1)	
Idap	Size	REG_DWORD	0x00000001 (1)	
b 🛄 lltdio 👻	Big SMB1	REG_DWORD	0x00000000 (0)	
4 I III +	4	111		

حال میتوانید ابزار ویرایش رجیستری را ببندید. همانند ویندوز ۸ و ۱۰، برای اینکه تغییرات انجام شده بر روی سیستم اعمال شوند، میبایست یک بار کامپیوتر خود را Restart کنید. اگر بنا به هر دلیلی تصمیم گرفتید که پروتکل SMBv1 را فعال نمایید، فقط کافی است به همین مسیر بروید و مقدار SMB1 را حذف نمایید.

<u>https://itresan.com/</u> : منبع