

## هشدار! هنگام ارتقاء یا بروزرسانی ویندوز ۱۰ کامپیوتر خود را رها نکنید

بیشتر کاربران یک عادت بد دارند که هنگام ارتقاء سیستم عامل ویندوز، آن را رها می کنند. البته این مسأله به این مربوط است که فرایند ارتقاء ویندوز ۱۰ طولانی و خسته کننده است. چرا این مسأله نگران کننده است؟

هنگام ارتقاء ویندوز ۱۰، یک شخص نزدیک به قربانی (یا حتی کسی که قربانی او را نمی شناسد) می تواند بدون نیاز به نرم افزار اضافی و با وجود اینکه BitLocker نصب است رابط خط فرمان را با دسترسی کامل باز کند و کارهای خرابکارانه انجام دهد. این مسأله به مایکروسافت گزارش شده است و این کمپانی در حال رفع این مشکل است.

هنگام ارتقاء ویندوز ۱۰، کلیدهای Shift + F10 را فشار دهید تا رابط خط فرمان با دسترسی root برایتان باز شود تا بتوانید BitLocker را دور بزنید!

اگر برای امنیت سیستم خود به نرم افزار کدگذاری Windows Bitlocker اعتماد کرده اید، پس آگاه باشید! چون کسی که به سیستم شما دسترسی فیزیکی دارد می تواند به اطلاعات شما دسترسی داشته باشد! کل کاری که لازم است هکر انجام دهد، فشار دادن همزمان کلیدهای Shift+F10 هنگام ارتقاء ویندوز ۱۰ است. محقق امنیتی Sami Laiho این روش دور زدن Bitlocker را کشف کرده است. وقتی شما در ویندوز ۱۰ در حال نصب یک سیستم عامل جدید هستید هکر می تواند با فشار دادن Shift+F10 رابط خط

فرمان (Command Line Interface) را با دسترسی های سیستمی باز کند. سپس با وجود فعال بودن BitLocker در سیستم قربانی، رابط خط فرمان دسترسی کامل هارد دیسک را به هکر می دهد. زیرا در زمان ارتقاء سیستم عامل، Windows PE (Pre-installation Environment) برای نصب ایمج جدید ویندوز مجبور است BitLocker را غیرفعال کند.

توجه شود که یکی از ویژگی های رفع مشکل ویندوز این است که به شما اجازه می دهد کلیدهای Shift+F10 را فشار دهید تا رابط خط فرمان برایتان باز شود. متأسفانه این ویژگی با غیرفعال کردن BitLocker، دسترسی به تمام اطلاعات هارد دیسک را در حین ارتقاء ویندوز ممکن می سازد.

بنابراین هکر برای سوءاستفاده نیاز به دسترسی فیزیکی کوتاه مدت به کامپیوتر هدف دارد، پس از آن به راحتی می تواند BitLocker را دور زده و دسترسی مدیر (Administrator) پیدا کند. مسئله ای که می تواند روی ابزارهایی که در حوزه اینترنت اشیاء از ویندوز ۱۰ استفاده می کنند تأثیر بگذارد.

### چگونه ریسک این خطر را کاهش دهیم؟

به عنوان اقدام متقابل، به کاربران توصیه می شود که در حین ارتقاء ویندوز خود آن را رها نکنند. همچنین می تواند به کاربران توصیه کرد از ویندوز ۱۰ نسخه LTSB استفاده کنند چون این نسخه از ویندوز ۱۰۰ به طور خودکار ارتقاء یا بروزرسانی انجام نمی دهد.

کاربران ویندوز ۱۰ می توانند با استفاده از SCCM (System Center Configuration Manager) دسترسی به رابط خط فرمان در حین ارتقاء ویندوز را مسدود نمایند. برای این کار در پوشه Setup\Scripts سیستم عامل، یک فایل با نام DisableCMDRequest.tag ایجاد کنند.

**اداره حراست آموزش شده شهید یزدانپناه سنندج**