禪

کارشناسان اعلام کردند :

اپلیکیشنهای اندرویدی مدیریت رمز عبور آلوده هستند!

جدیدترین پژوهش انجام شده از سوی کارشناسان امنیتی نشان میدهد اطلاعات شخصی کاربران ممکن است در معرض تهدید جدی قرار داشته باشد . در این پژوهش، محققان نه نرمافزار مدیریت کننده گذرواژههای عرضه شده ویژه پلتفرم اندروید را مورد بررسی قرار داده و اعلام کردهاند این نرمافزارها به رخنههای جدی آلوده هستند .

اگر روی گوشی هوشمند خود از یک نرمافزار مدیریت گذرواژهها برای ذخیرهسازی اطلاعات مربوط به لاگین کردن به سایتها استفاده میکنید، ممکن است در معرض یک تهدید امنیتی بزرگ قرار داشته باشید . پژوهشگران امنیتی مدعی شدهاند آسیبپذیریهای جدی را در تعدادی از نرمافزارهای محبوبی که ویژه اندروید عرضه شدهاند شناسایی کردهاند . رخنههایی که ممکن است اطلاعات کاربران را افشا کنند .

نرمافزارهای مدیریت کننده گذرواژهها از یک برنامه مرکزی برای ذخیرهسازی اطلاعات هویتی که ترکیب نام کاربری و گذرواژها است، استفاده میکنند . اطلاعاتی که برای ورود به سایتها و سرویسهای مختلف مورد نیاز است . این برنامهها به کاربران اجازه میدهند در مراجعات بعدی به سایتهای موردنظر خود بدون آنکه نیازی به وارد کردن این جزییات داشته باشند، به طور مستقیم به سایتها و سرویسها وارد شوند. در این حالت نرمافزار به طور خودکار فیلدهای مربوطه را پر کرده و مقداردهی میکند . در این مکانیزم کاربران تنها باید گذرواژه اصلی که به نام Master از آن یاد میشود را حذف کنند .

[illegible]

[illegible]

[illegible]

[illegible] LastPass 1Password, My [illegible] Passwords, Dashlane Password Manager, Informaticore's Password Manager, F-Secure KEY, [illegible] Avast Passwords ، Keepsafe, Keeper [illegible] master [illegible].

[illegible]

[illegible]

[illegible]!

[illegible] "[illegible]" [illegible].

[illegible] VPN [illegible].

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
16:12 - 14/12/1395
[illegible]:
[illegible] - [illegible] - password Manager - [illegible] - [illegible] - [illegible] - [illegible]