نحوه بایپس کدملی بخش پروفایل panel.idpay.ir در جهت TakeOver کردن کدملی های کاربران

شکارچی	شناسه گزارش	تاریخ ثبت	ویدیو / عکس
TODO	TODO	2021-11-28	TODO

شرح آسیب پذیری (شکارچی)

باسلام قبلا نمونه این آسیب پذیری در گزارش pr2021-08-20-0001 آورده شد که داپلیکیت شد و نحوه عملکرد اون بگونه ای است که هنگام ثبت نام از متقاضی برای احراز هویت نیاز به کدملی می باشد که این امر از الزامات فیلد کدملی است ودرصورت اشتباه خطا میداد ولی این آسیب پذیری نیز در بخش دیگری موجود هست ؛ بخش پروفایل ها به ادرس https://panel.idpay.ir/profiles/ که سوای موقع ثبت نام است و با مکانیزم بیشتر در دسترس هست و مهاجم می تواند پروفایل های مختلفی با کدملی های مختلف ایجاد کند در ویدیو در پنل چند مورد دیگر برای تست ثبت شده است که می توان کدملی های مختلفی را TakeOver کرد حال ساختار فیلد کدملی یک سری کتابخانه و الگوریتم آماده هست که براحتی قابل بایپس هست و میتواند با No Rate Limit تعداد زیادی کدملی فعال استخراج کرد بنابراین مهاجم با یک شماره موبایل و کدملی های مختلف می تواند لاگین شود که همه کدملی های به یک شماره متصل باشند که بعد از آن دیگر کاربران آیدی پی برای ثبت نام نتوانند از کدملی خود استفاده کنند با این اوصاف در ویدیو از یک کد ساده شبیه موبایل استفاده گردید (برای اینکه نقض حریم خصوصی نشده باشد از کدملی واقعی استفاده نشد) که با تغییر هر عدد می توان کد فعال را پیدا کرد و یک اکانت پروفایل ایجاد کرد و با آن لاگین شد . بااحترام /.

چگونه می‌توان آسیب‌پذیری را رفع کرد ؟ (شکارچی)

تماس با راورو :

دفتر مرکزی تهران، خیابان مطهری، نبش سهروردی، پلاك ۹۴ ، طبقه دوم، واحد ۲۵۰

شماره تماس 021-9103-1553

شماره فکس 021-9103-1553

آدرس ایمیل support[at]Ravro[dot]ir