# قوانین

از تمامی علاقمندان، متخصصان، پژوهشگران امنیت و هکر‌ها دعوت‌ می‌شود تا با ارایه گزارش‌ آسیب‌پذیری از سرویس‌های مجموعه جیبرس به ما در حفظ و ارتقا امنیت سامانه‌هایمان کمک کنند. لازم به‌ذکر است، گزارش‌هایی که مطابق با قوانین و توضیحات مندرج در اهداف باشند و همچنین در محدوده‌ی مجاز قرار بگیرند، پس از ارزیابی فنی تیم داوری مورد تایید قرار گرفته و می‌تواند شامل پرداخت شود. به ازای هر گزارش تایید شده، ضریب تاثیرگذاری آسیب‌پذیری‌ بر اساس استاندارد CVSS v3 محاسبه می‌گردد و مبلغ قابل پرداخت با توجه به ضریب تاثیرگذاری و نوع دسته‌بندی آسیب‌پذیری تعیین می‌گردد.

حداکثر مدت زمان بررسی گزارش توسط میدان: ۱۵ روز کاری

حداکثر مهلت پرداخت پس از تایید گزارش: ۱۰ روز کاری

# توضیحات عمومی

دستورالعمل شناسایی شدت آسیب‌پذیری

تمامی گزارش‌های ارسالی به جیبرس در مقیاسی هدفمند و ساده ارزیابی می‌شوند. هر کدام از آسیب‌پذیری‌ها منحصربفرد هستند، اما دستورالعمل زیر به‌شکلی واضح به ما برای ارزیابی و دسته‌بندی شدت آسیب‌پذیری کمک می‌کند. در حال حاضر ما تنها برای گزارش‌های سطح بالا و بحرانی جایزه در نظر گرفته‌ایم.

مرگ و زندگی

در سطح مرگ و زندگی یک فاجعه غیرقابل بازگشت می‌تواند رخ دهد. شما درباره مرگ و زندگی می‌توانید تصمیم بگیرید و دسترسی برای کنترل همه چیز دارید. دسترسی برای ایجاد تغییر در تمامی بخش‌های کدها، ای‌پی‌آی، دیتابیس و فایل‌های جیبرس و کلیه مشتریان در این سطح رخ می‌دهد.

بحرانی

مشکلات بحرانی پی‌آمدهای مستقیم و فوری را برای جیبرس یا طیف وسیعی از کاربران ما ایجاد می‌کنند. این موارد غالبا در زیرساخت‌های ما یا اجزایی از برنامه‌های کاربردی سطح پایین و اثرگذار در سرویس‌های ما هستند.

بالا

مشکلات شدید پی‌آمدهای مثل اجازه دسترسی به مهاجم برای خواندن یا ویرایش داده‌های با حساسیت بالا را که به آن دسترسی ندارد ممکن می‌کند. از نظر وسعت معمولا این مشکلات محدودتر از مشکلات بحرانی هستند، اگرچه ممکن است هم‌چنان دسترسی گسترده‌ای را در اختیار مهاجمان قرار دهند.

متوسط

مشکلات متوسط معمولا به مهاجم اجازه خواندن یا ویرایش بخش محدودی از داده‌ها را که به آن دسترسی ندارند می‌دهد. معمولا این دسترسی‌ها به داده‌های با حساسیت کمتر از سطح شدید منجر می‌شوند.

کم

مسائل مربوط به شدت کم به شکل معمول به مهاجم اجازه می‌دهند تا به بخش به شدت محدودی از داده‌ها دسترسی پیدا کند. در این سطح معمولا چگونگی رفتار یک بخش نقض شده و خارج از انتظار عمل می‌کند، اما این امر تقریبا امکان افزایش دسترسی یا توانایی برای رفتار ناخواسته را برای مهاجم فراهم نمی‌کند.

توجه داشته باشید که تنها آسیب‌پذیری‌های شامل اکسپلویت بررسی خواهند شد.

۱. از اختلال در عملکرد و فرآیند‌های سامانه‌‎های مجموعه جیبرس اجتناب کنید.

۲. در هر گزارش فقط یک آسیب‌‌‎پذیری ارایه شود.

۳. شرح آسیب‌‎پذیری بصورت کامل به همراه شدت و خطرات احتمالی توضیح داده شود.

۴. از آدرسIP مشخصی برای بررسی و ارزیابی استفاده کنید و IP آدرس مذکور را در گزارش اعلام کنید.

۵. تمام فعالیت‌‎ها و دسترسی‌ها می‌‎بایست در گزارش قید شود.

۶. مراحل باز‌ تولید آسیب‌‎پذیری بطور کامل شرح داده شود.

۷. مستندات لازم (تصاویر، فیلم، کدها، PoC و...) جهت دسترسی و استفاده از آسیب‌‎پذیری به همراه ابزارهای لازم به‌‎طور کامل بارگذاری شود.

۸. هرگونه تنظیم خاص مورد نیاز برای بازسازی حمله، باید ارایه شود.

۹. از بارگذاری مستندات آسیب‎پذیری‎ها در سایت‌های اشتراکی، شبکه‌های اجتماعی و ... اجتناب شود.

۱۰. به حریم شخصی افراد و کاربران احترام گذاشته شود و هیچگونه تعاملی با حساب کاربری افراد، بدون رضایت آن‌ها انجام ندهید. برای تست عملکرد آسیب‌پذیری‌های مربوط به حساب کاربری، باید از حساب کاربری خود استفاده کنید.

۱۱. اطلاعات محرمانه نباید افشا شود و پس تایید گزارش می‌‌‎بایست از نگهداری آن‌ها اجتناب کنید.

۱۲. قبل از زمان مشخص شده جهت بررسی و حل مشکل گزارش شده و بدون هماهنگی و کسب اجازه از مجموعه جیبرس، هیچگونه اطلاعاتی در مورد مشکل را عمومی نکرده و با دیگران به اشتراک نگذارید.

۱۳. از مشکلات امنیتی‌ که یافته‌اید، به هیچ عنوان، بهره‌برداری و سوءاستفاده نکرده‌ باشید/نکنید.

۱۴. هیچ‌یک از موازین قانونی کشور را زیر پا نگذاشته باشید.

۱۵. آسیب‌پذیر‌ی‎های گزارش شده می‎بایست تاثیر مشخصی بر کاربران، سامانه‌‎ها یا داده‎های مجموعه جیبرس داشته باشد.

۱۶. دریافت پاداش به معنی مجوز جهت افشای گزارش نمی‌باشد و هرگونه افشای گزارش منوط به هماهنگی با مجموعه جیبرس می‌باشد.

۱۷. مبنا‌ی محاسبه‌ی شدت آسیب‌پذیری‌ها استاندارد CVSS v3 می‌باشد.

۱۸. جهت تست عملکرد آسیب‌پذیر‌ی‌های مرتبط به حساب کاربری، تنها مجاز به استفاده از حساب کاربری خود هستید.

۱۹. ثبت گزارش آسیب‌پذیری به معنای مطالعه‌ و پذیرش قوانین می‌باشد.

حداکثر مدت زمان بررسی گزارش توسط میدان ۱۵ روز کاری

حداکثر مهلت پرداخت پس از تایید گزارش ۱۰ روز کاری

# محدوده مجاز

وب‌سایت جیبرس براساس الگوی دامنه‌های زیر می‌باشد

https://\*.jibres.ir

https://\*.talambar.ir

https://\*.jibres.com

[https://\*.talambar.com](https://*.talambar.com)

# محدوده غیرمجاز

اپلیکیشن اندروید جیبرس و اپلیکیشن اندروید مشتریان جیبرس جز محدوده غیرمجاز محسوب می‌شود.

تمامی سرویس‌ها و خدمات سایر شرکت‌ها که در وب‌سایت یا اپ جیبرس و مشتریان مورد استفاده قرار گرفته، جز محدوده‌ی غیرمجاز محسوب می‌شود.

# شرایط پرداخت

حداقل پرداخت به ازای گزارش‌های آسیب‌پذیری شامل پاداش، مبلغ ۱۰۰,۰۰۰ تومان (به حروف صد هزار تومان)

حداکثر پرداخت به ازای گزارش‌های آسیب‌پذیری شامل پاداش، مبلغ ۱۰,۰۰۰,۰۰۰ تومان (به حروف ده میلیون تومان)

امتیاز و مبلغ نهایی بر اساس شدت تاثیرگذاری و بر اساس قوانین هدف محاسبه خواهد شد.

# آسیب‌پذیری‌های قابل قبول

سطح مرگ و زندگی: حداکثر پرداخت مبلغ ۱۰,۰۰۰,۰۰۰ تومان (به حروف ده میلیون تومان)

سطح بحرانی: حداکثر پرداخت مبلغ ۲,۰۰۰,۰۰۰ تومان (به حروف دو میلیون تومان)

۱. آسیب‌پذیری‌هایی که منجر به دسترسی به اطلاعات خصوصی مشتریان جیبرس شود. (بدست آوردن و یا دامپ گرفتن اطلاعات مشتریان)

۲. آسیب‌پذیری‌هایی که منجر به تداخل و یا تغییر در فرآیند‌های خدمات جیبرس شود. (مثل تغییر بسته‌های خریداری شده)

۳. آسیب‌پذیری‌هایی که منجر به دسترسی به حساب کاربری مشتریان جیبرس شود.

سطح بالا: حداکثر پرداخت مبلغ ۱,۰۰۰,۰۰۰ تومان (به حروف یک میلیون تومان)

۱. آسیب‌پذیری‌هایی که منجر به دور زدن مکانیزم‌های احراز هویت در جیبرس شود.

۲. آسیب‌پذیری‌هایی که منجر به تداخل، تغییر و یا سوء استفاده در تراکنش‌های مالی جیبرس شود.

۳. آسیب‌پذیری‌هایی که منجر به دیفیس یا تغییر در صفحه‌ی اصلی وب‌سایت جیبرس شود.

سطح متوسط: حداکثر پرداخت مبلغ ۵۰۰,۰۰۰ تومان (به حروف پانصد هزار تومان)

# آسیب‌پذیری‌های غیر قابل قبول

۱. آسیب‌پذیری‌هایی که به تعامل با کاربر نیاز داشته باشد شامل حملات Phishing و ...

۲. آسیب‌پذیری‌هایی که قبلاً توسط سایر متخصصین گزارش شده باشد.

۳. آسیب‌پذیری‌هایی که در دامنه ها و آدرس های IP غیر از محدوده‌ مجاز هدف باشد.

۴. گزارش‌های ارائه شده توسط اسکنر‌ها و سایر ابزار‌های اتوماتیک، بدون ارایه اکسپلویت.

۵. آسیب‌پذیری‌های مربوط به نشت اطلاعات سرور و پیکربندی نادرست آن، مثل نسخه و نوع وب سرور.

۶. آسیب‌پذیری‌های مربوط به SSLو Best Practice های‌ مربوط به آن.

۷. آسیب‌پذیری‌های مربوط به مرورگرهای قدیمی.

۸. آسیب‌پذیری‌های مربوط به حملات فیزیکی.

۹. آسیب‌پذیری‌های Clickjacking.

۱۰. آسیب‌پذیری‌های self\*.

۱۱. حملات Brute Force به غیر از موارد مربوط به Captcha.

۱۲. حملات مهندسی اجتماعی و Phishing.

۱۳. حملات از كار اندازی سرویس (DoS/DDoS).

۱۴. Best Practiceها، شامل حداقل طول كلمات عبور و غیره.

۱۵. نامه نگاری الکترونیکی جعلی (E-mail spoofing).

۱۶. گزارش پایین بودن ورژن کتابخانه‌ها و نرم افزار‌های به کار برده شده.

۱۷. هر مورد مربوط به بدست آوردن نام‌های کاربری با استفاده از (Account/e-mail enumeration).