قوانین

همه فناوری‌ها دارای اشکال و باگ هستند. اگر یک آسیب‌پذیری امنیتی یافتید، مایلیم تا به شما کمک کنیم تا آن را به شکل صحیح با ما در جریان بگذارید. ارسال گزارش آسیب‌پذیری در برنامه گزارش باگ جیبرس مهیا شده است. اثبات مفهوم مهم‌ترین بخش در ارسال گزارش است. مراحل شفاف و تکرارپذیر به ما کمک می‌کند تا با سرعت بیشتری مشکل را اعتبارسنجی کنیم.

بدین‌وسیله از تمامی علاقمندان، متخصصان، پژوهشگران امنیت و هکرها دعوت می‌شود تا با ارایه گزارش آسیب‌پذیری از سرویس‌های 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 جیبرس ۱۵ روز کاری می‌باشد.

- حداکثر طی ۱۰ روز کاری پس از تایید گزارش، باگ‌بانتی پرداخت خواهد شد.

توضیحات عمومی

فلسفه افشای آسیب پذیری

- به حریم خصوصی احترام بگذاریم. لطفا حسن نیست داشته باشید و از داده‌های کاربران دیگر سوء استفاده نکنید یا برای از بین بردن آن‌ها تلاش نکنید.

- صبور باشید. لطفا گزارش‌های خود را به‌صورت شفاف و همراه با جزئیات ارسال کنید تا در مدت زمان پاسخ‌دهی ما را کاهش دهید.

- آسیب نزنید. از طریق ارسال گزارش‌های سریع، آسیب‌پذیری‌های یافت شده را گزارش کنید. هرگز بدون اجازه از داده‌های کسی استفاده نکنید.

باگ یا اشکال نرم‌افزاری به مهاجمان این امکان را می‌دهد تا با نقض خط مشی امنیتی نسبت به نفوذ اقدام کنند. نقص در طراحی یا عدم رعایت بهترین شیوه‌های امنیتی ممکن است به‌عنوان آسیب‌پذیری شناخته شود. نقاط ضعف مورد استفاده توسط ویروس‌ها، کدهای مخرب و مهندسی اجتماعی، آسیب‌پذیری محسوب نمی‌شوند.

اگر فکر می‌کنید که یک آسیب پذیری از جیبرس پیدا کرده‌اید، لطفا گزارش آن را در اینجا برای ما ثبت کنید. گزارش باید شامل شرح مفصل و روشنی از مورد کشف‌شده باشد، مراحل کوتاه و قابل تکرار و یا اثبات مفهوم کار باشد. اگر شما جزئیات آسیب‌پذیری را به‌درستی شرح ندهید، ممکن است تاخیر قابل توجهی در فرایند گزارش افشا بوجود بیاید که برای همه نامطلوب است. ما برای محاسبه کیفیت آسیب‌پذیری در جیبرس از استاندارد CVSS v.3 استفاده خواهیم کرد.

قبل از شروع

- هرگز حملات غیر فنی مانند مهندسی اجتماعی، فیشینگ یا حملات فیزیکی علیه کارکنان، کاربران یا زیرساخت های ما را امتحان نکنید!

- هنگامی که در شک بودید، با ما از طریق آدرس ایمیل info [at] jibres.com تماس بگیرید.

- با شرکت در برنامه گزارش باگ جیبرس، شما تصدیق می‌کنید که شرایط استفاده از خدمات جیبرس را خوانده و موافقت خود را با آن اعلام کرده‌اید.

- مشارکت شما در این برنامه، هیچ‌گونه قانون قابل اجرا علیه شما را نقض نمی‌کند و اجازه انتشار، استفاده، مصالحه یا مختل کردن داده‌هایی که برای شما نیست را به شما نمی‌دهد.

- فقط تست آسیب‌پذیری در سایت‌های جیبرس در محدوده مجاز بررسی هستند. برخی از سایت های میزبانی شده در زیردامنه‌های جیبرس توسط اشخاص ثالث اداره می‌شود و نباید آزمایش شود.

- جیبرس این حق را برای خود محفوظ می‌داند که به صلاحدید خود برنامه گزارش باگ را فسخ کرده یا به آن ادامه ندهد.

- تا زمانی که جیبرس این باگ را ارزیابی نکرده است، تقاضا و گزارش خود را علنی نکنید.

پژوهش خود را انجام دهید

سایر کاربران را با آزمایش‌های خود تحت تاثیر قرار ندهید. برای مثلا اگر می‌خواهید یک دور زدن مجوز اعتبارسنجی را دور بزنید، باید از حساب کاربری خودتان استفاده کنید.

موارد زیر هرگز مجاز نبوده و طبیعتا واجد دریافت پاداش نیز نیستند. هم‌چنین ممکن است ما به دلیل انجام این کارها حساب کاربری شما را به حالت تعلیق درآوریم و آدرس آی‌پی شما را مسدود کنیم.

- انجام حملات محروم‌سازی از سرویس یا دی‌داس DDoS یا سایر حملات حجمی.

- محتوای هرزنامه

- اسکنرهای مخاطرات امنیتی، خزنده‌ها یا ابزارهای خودکار در مقیاس بزرگ که باعث ایجاد ترافیک زیاد می‌شوند.

- **توجه** تا زمانی که ابزارهای خودکار منجر به ایجاد حجم ترافیکی زیاد نشوند ما مجاز به استفاده از آن‌ها هستیم. برای مثال اجرای یک اسکن nmap برای یک هاست مجاز است اما ارسال ۱۰.۰۰۰ درخواست در یک دقیقه توسط برپ سوییت قطعا بیش از اندازه است.

لطفا نکات زیر را درنظر داشته باشید

۱. از اختلال در عملکرد و فرآیندهای سامانه‌های 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 آدرس IP 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 به‌طور کامل شرح داده شود.

۷. مستندات لازم شامل تصاویر، فیلم، کدها، PoC 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.

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 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 جیبرس داشته باشد.

۱۶. دریافت پاداش به معنی مجوز جهت افشای گزارش نمی‌باشد و هرگونه افشای گزارش منوط به هماهنگی با جیبرس پس از رفع باگ 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 گزارش باگ جیبرس می‌باشد.

۲۰. اگر فکر می‌کنید که دسترسی به خدمات با انجام این کار تحت تاثیر قرار می‌گیرد و از دسترس خارج می‌شود، بلافاصله عملیات را متوقف کنید. در مورد نشان دادن تاثیر کامل آسیب‌پذیری پیدا شده، نگران نباشید. تیم امنیتی جیبرس قادر به تعیین میزان تاثیرگذاری خواهند بود.

۲۱. با توجه به گسترگی بخش‌های مختلف جیبرس و اینکه به‌شدت در حال توسعه محصول بوده و روزانه بخش‌های زیادی از سیستم تغییر کرده یا بروزرسانی می‌شوند. گزارش‌هایی ممکن است در این بخش‌ها اعلام شوند که برای این موارد، ما زمان اعلام نظر تیم داوری راورو را درنظر میگیریم و اگر پیش از بررسی تیم داوری تغییراتی در آن زمینه رخ داده باشد، باید پس از تغییر هم مشکل پابرجا باشد.

۲۲. از آنجایی که برنامه گزارش باگ جیبرس بر روی وب‌سایت جیبرس هم فعال هست، گزارش‌های ثبت شده روی جیبرس و راورو، بر اساس زمان ثبت اولیه بررسی شده و تکراری بودن آن بررسی می‌گردد.

۲۳ .آسیب‌پذیری‌هایی که راه‌حل مشخصی برای رفع آن وجود ندارد، مورد قبول نمی‌باشد.

۲٤ .گزارش‌های دریافتی حداکثر در ۱۵ روز کاری توسط جیبرس بررسی خواهند شد.

۲۵. پس از تایید گزارش، بانتی درنظر گرفته شده حداکثر تا ۱۰ روز کاری پرداخت می‌گردد.

محدوده مجاز

وب‌سایت اصلی جیبرس براساس الگوی دامنه‌های زیر می‌باشد.

- https://*.jibres.ir

- https://*.jibres.com

وب‌سایت مشتریان جیبرس تا پیش از اتصال به دامنه اختصاصی در آدرس‌های زیر می‌باشد

- https://*.jibres.store

- https://*.myjibres.com

فایل‌های جیبرس بر روی آدرس زیر می‌باشد.

- https://*.talambar.ir

- https://*.talambar.com

محدوده غیرمجاز

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

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

شرایط پرداخت

مبنای محاسبه‌ی شدت آسیب‌پذیری‌ها استاندارد CVSS v3 می‌باشد. امتیاز و مبلغ نهایی **بر اساس سطح و شدت تاثیرگذاری** و بر اساس قوانین هدف محاسبه خواهد شد. بدین مفهوم که ابتدا سطح آسیب‌پذیری شناسایی شده، سپس شدت به‌عنوان ضریب اعمال می‌شود.

- سطح مرگ و زندگی	حداکثر پرداخت **مبلغ ۱۰,۰۰۰,۰۰۰ تومان**
- سطح بحرانی	حداکثر پرداخت **مبلغ ۵,۰۰۰,۰۰۰ تومان**
- سطح بالا	حداکثر پرداخت **مبلغ ۲,۰۰۰,۰۰۰ تومان**
- سطح متوسط	حداکثر پرداخت **مبلغ ۵۰۰,۰۰۰ تومان**
- سطح پایین	حداکثر پرداخت **مبلغ ۱۰۰,۰۰۰ تومان**

در بخش **آسیب‌پذیری‌های قابل قبول** جزئیات دقیق هریک از سطوح ذکر شده است.

آسیب‌پذیری‌های قابل قبول

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 سطح آسیب‌پذیری کمک می‌کند.

به‌دلیل وجود دامنه‌های متفاوت و نقاط نهایی گوناگون، آسیب‌پذیری‌های مشابه در صفحات و آدرس‌ها و بخش‌های متفاوت، یکسان بوده و تکراری درنظر گرفته می‌شوند.

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

سطح حیاتی یا مساله 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.

1. Business Destruction Vulnerability
2. RCE on all servers

سطح 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.

1. SQL/NoSQL/Command Injection
2. Remote Command Execution
3. Mass DNS takeover
4. Mass Account Takeover without User Interaction
5. XML External Entity Injection
6. Sensitive Data Exposure to Accessible Services like Password, Private API Keys, SSL private Keys of Jibres
7. RCE on vital servers

سطح 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.

1. Unauthorized Access to Read and Write Sensitive Data of a User
2. Weak Password Reset Implementation
3. Unauthorized Access to Read and Write Part of Sensitive Data of all User
4. Local File Inclusion

5. SSRF with Internal High Impact

6. Complete Source Code Disclosure

7. Privilege Escalation to Admin Account

8. Mass delete users Accounts

9. Authentication Bypass

10. Sensitive Data Exposure of all users

سطح 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.

1. Partial Source Code Disclosure

2. SSRF (Internal Scan and/or Medium Impact)

3. Unauthorized Access to Read and Write Part of Sensitive Data of a User

4. OAuth mis usable misconfiguration

5. CRLF Injection

6. Unauthorized Access to Services (API / Endpoints)

7. DOM based XSS

8. Mis usable misconfiguration of CAPTCHA implementation

9. Delete a user Account

10. State Changing CSRF

11. Source Code Disclosure of Jibres websites

12. Insecure Direct Object Reference

13. Reflected XSS

14. Second Factor Authentication (2FA) Bypass

15. Authorization Bypass

16. Default credentials

17. DoS (High Impact and/or Medium Difficulty)

18. Sensitive Data Exposure

19. Server-Side Request Forgery

20. Session Fixation (Remote Attack Vector)

21. Mass User Enumeration

22. iframe Injection

23. Clickjacking (Sensitive Click-Based Action)

24. Account Takeover by User Interaction

25. Blind XSS

26. Stored XSS

27. Excessively Privileged User / DBA

28. Sensitive Data Exposure of some users

سطح پایین

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.

1. Logical bug
2. Open redirect
3. Rate limit takeover
4. Inject from Editor
5. HTML injection
6. Security tips
7. IP Block takeover
8. Find Server IP

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.

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

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

٦. آسیب‌پذیری‌های مربوط بهSSL و Best Practice های مربوط به آن.

۷. آسیب‌پذیری‌های مربوط به مرورگرهای قدیمی.

۸. آسیب‌پذیری‌های مربوط به حملات فیزیکی.

۹. آسیب‌پذیری‌هایClickjacking.

۱۰. آسیب‌پذیری‌هایself*.

۱۱. حملات Brute Force

۱۲. حملات مهندسی اجتماعی وPhishing.

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

۱٤. موارد Best Practiceها، شامل حداقل طول کلمات عبور و غیره.

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

۱٦. 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).

۱۸. آسیب‌پذیری‌هایی مربوط به دیکامپایل کردن (decompile) فایل برنامه.

۱۹. آسیب‌پذیری‌هایی که تاثیر آن تنها بر سمت دستگاه کاربر (Client) باشد.

۲۰. آسیب‌پذیری‌های مربوط به.Captcha

۲۱. تمامی آسیب‌پذیری‌های مربوط به.Denial of service or rate limiting issues

۲۲. تمامی آسیب‌پذیری‌های مربوط به.Email validation not enforced

۲۳. تمامی آسیب‌پذیری‌های مربوط به SSL/TLS Issues such as: BEAST, BREACH, SSL...
insecure cipher suites enabled.

۲٤. تمامی آسیب‌پذیری‌های مربوط به.Cookie valid after password change/reset

۲۵. تمامی آسیب‌پذیری‌های مربوط به.Domain authentication

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

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

28. Missing Certification Authority Authorization (CAA) Record

29. Public Admin Login Page

30. Unsafe File Upload

31. Directory Listing Enabled (Non-Sensitive Data Exposure)

32. Crowdsourcing/OCR Captcha Bypass

33. Lack of Verification/Notification Email

34. Same-Site Scripting

35. Allows Disposable Email Addresses for Registration

36. Open Redirect (POST-Based)

37. Exposed Admin Portal to Internet

38. Lack of Security Headers

39. Missing DNSSEC

40. SSRF (DNS Query Only)

41. Concurrent Logins

42. Reflected File Download (RFD)

43. Http Parameter Pollution

44. Token Leakage via Referrer

45. Session Fixation (Local Attack Vector)