|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| الف- شناسنامه (مشخصات) آسيب پذيري | نام/CVE آسيب پذيري: | | | فرم شماره دو  نسخه اول |
| آدرس آی پی استفاده شده ارزیاب: | | |
| نوع ارزیابی:  🞏Black-Box 🞏Grey-Box 🞎White-Box | | | ارزیاب: |
| شدت آسیب پذیری بر اساس CVE3 | | | تاريخ ارزیابی: |
| بعد امنيتي نقض شده در صورت استفاده از آسيب پذيري:  🞏محرمانگي 🞏صحت 🞎دسترس پذيري 🞎تصديق هويت  🞏کنترل دسترسي امنيت ارتباط 🞏 حريم خصوصي 🞏 عدم انکار | | | |
| موقعيت ارزياب (منبع تهديد بهره بردار از آسيب پذيري):  🞏 دسترسي از روي سيستم 🞎 دسترسي از شبکه داخلي 🞏 دسترسي از بيرون (اينترنت) | | | |
| کنترل موثري در مقابل بهره برداري از آسيب پذيري:  🞏 وجود دارد 🞏 وجود ندارد | | | |
| تکنيک تشخيص آسيب پذيري:  🞏 تکنيک مرور اطلاعات  🞏تکنيک شناسايي و تحليل وضعيت  🞏 تکنيک اعتبارسنجي  🞏 روش تست نفوذ  🞏 جمع آوري اطلاعات 🞏 تست مديريت پيکربندي 🞏 تست احراز هويت  🞏 مديريت نشست 🞎 تعيين سطح دسترسي 🞏 تست منطق کسب و کار  🞎 اعتبارسنجي داده ها 🞏 اخلال در سرويس دهي 🞏 تست خدمات وب  🞏 تستAjax  🞎 با استفاده از شکستن رمز عبور  🞏 مهندسي اجتماعي | | | |
| **شرح آسيب پذيري:**  **شواهد آسیب پذیری: (**شامل تصاویر، Payload، توضیح مرحله به مرحله سناریو; درصورت نیاز ویدیو ارسال شود**)**  **ارایه راه حل پیشنهادی (**اختیاری**)** | | | |
| ب- تحليل مخاطره آسيب پذيري | | ميزان ضربه فني در صورت بهره برداري منبع تهديد از آسيب پذيري:  🞏زياد 🞎 متوسط 🞎 کم | | |
| * ميزان نقص محرمانگي اطلاعات:   🞏 افشاي اندک داده­هاي حساس  🞏 افشاي اندک داده­هاي غير حساس  🞎 افشاي اندک داده­هاي حياتي  🞏 افشاي بسياري از داده­هاي حساس  🞏 افشاي بسياري از داده­هاي غيرحساس  🞏 افشاي تمام اطلاعات یا افشاي بسياري از داده­هاي حياتي   * ميزان نقص صحت داده:   🞏 تحريف اندک بخش کمي از داده­ها  🞏 تحريف جدي بخش کمي از داده­ها  🞏 تحريف اندک بخش زيادي از داده­ها  🞎 تحريف جدي بخش زيادي از داده­ها  🞏 تحريف کامل داده­ها   * ميزان نقص دسترسي سرويس:   🞏 اختلال اندک در سرويس­هاي جانبي  🞎 اختلال اندک در سرويس­هاي اصلي  🞏 اختلال وسيع در سرويس­هاي جانبي  🞏 اختلال وسيع در سرويس­هاي اصلي   * ميزان رديابي اقدامات مهاجم:   🞏 کاملا قابل رديابي است  🞏 امکان رديابي وجود دارد  🞏 قابل رديابي نيست- کاملا ناشناس | | |
|  | | احتمال بهره برداري منبع تهديد از آسيب پذيري: 🞏 زياد 🞎 متوسط 🞏 کم | | |
| فاکتورهاي عامل تهديد:   1. ميزان مهارت فني مهاجم:   🞏 بدون مهارت فني  🞎 مهارت فني محدود  🞎 کاربر پيشرفته کامپيوتر  🞏 داراي مهارت برنامه نويسي و شبکه  🞏 داراي مهارت نفوذ   1. انگيزه و منفعت مهاجم در کشف و بهره­برداري از آسيب­پذيري:   🞎 بدون منفعت يا منفعت کم  🞎 منفعت متوسط  🞏 بسيار پر منفعت   1. فرصت و شانس دسترسي مهاجم در کشف و بهره­برداري از آسيب پذيري:   🞏 بدون دسترسي  🞎 دسترسي محدود  🞏 دسترسي کامل   1. ميزان گستردگي گروه مهاجم:   🞏 توسعه­دهنده سيستم  🞏 مدير سيستم  🞎 کاربر شبکه داخلي  🞏 شرکا  🞏 کاربران مجاز  🞏 کاربران اينترنت | فاکتورهاي آسيب پذيري:   1. سهولت کشف آسيب­پذيري براي مهاجم:   🞏 تقريبا غير ممکن  🞎 سخت  🞏 آسان  🞏 در دسترس بودن ابزارهاي خودکار   1. سهولت بهره­برداري از آسيب پذيري براي مهاجم:   🞎 بطور نظري قابل انجام است  🞎 سخت  🞏 آسان  🞏 در دسترس بودن ابزارهاي خودکار   1. ميزان شناخته شده بودن آسيب پذيري براي مهاجم:   🞏 ناشناخته  🞎 پنهان  🞏 واضح  🞏 کاملا شناخته شده | |
| ميزان مخاطره: 🞏 زياد 🞎 متوسط 🞎 کم | | |