سعود أ بوشيبه | Saud
SaudSubaie_@

14 تغريدة • UTC 15:59:42 16-06-2020 • اقرأها في تويتر
rattibha.com

#ثريد بتكلم فيه عن الثغرات وأنواعها بإختصار :

Vulnerabilities

هي عبارة عن نقاط ضعف في الوسائل التقنية أو الأنظمة والشبكات وتكون معرضة للإختراق في أي وقت سواءً كانت بأخطاء بشرية أو تقنية ، يوجد العديد من نقاط الضعف ذكرت بعضاً منها

#أمن_المعلومات
#الامن_السيبراني

: Vulnerability types

- Race condition

هي عبارة عن عمليتين او أكثر حصلت في وقت واحد .
ومثال عليها عندما تريد تحويل مبلغ وبنفس الوقت يوصلك مبلغ محول لك فهذه ممكن تكون نقطة ضعف في النظام.

- End -of-life vulnerabilities

تحصل هذه الثغرة عندما يتوقف الدعم عن البرنامج او النظام. مثل : عندما تستخدم نظام تشغيل قديم تكون هناك نقاط ضعف لأن الدعم تم إيقافه من الشركة المصنعة

- Improper input handling

هناك أنواع من الاستغلال تنتج عن عدم التحقق من صحة المدخلات ويسبب هجمات Buffer overflows ومع التعامل الصحيح مع المدخلات سوف يحد ذلك من الاستغلال والقضاء عليه.

- lmproper error handling

عند حدوث خطأ ما وعدم التعامل المناسب معه من قبل النظام او البرنامج بحيث يعطي معلومات اكثر من اللازم عن الخطأ فقد يسمح ذلك بتوليد نقطة ضعف ينتج عنه تسريب للمعلومات الأساسية للمهاجم او الكشف عن ضعف او تفاصيل حول خلل ما يمّكن المهاجم من اختراقه.

- Misconfiguration / weak configuration

اذا كانت هنالك اخطاء في الإعدادات فهذه من الثغرات التي يمكن للمهاجم استغلالها ، أو تكون الإعدادات ضعيفه فهذه نقطة ضعف. مثلاً : عندما تقوم بجعل المستخدمين يعلمون Authentication وتكون بدون قيود مما يجعل المستخدمين يضعون باسورد ضعيف .

Default configuration -

غالب الأجهزة والأنظمة تأتي بإعدادات إفتراضية من المصنع كأسم المستخدم والباسورد ، يفترض أمنياً عندما تريد تركيب جهاز أن تقوم بحذف وتغيير الإعدادات الافتراضيه لأنها تكون معروفة للجميع وتكون أيضاً في موقع الشركة مما يسهل على المهاجم البحث عن معلوماتها.

Untrained users-

من خلال المستخدمين الغير مدربين يمكن ان يكون هناك نقطة ضعف بحيث يرتكبوا اخطاء أمنية او إساءة استخدام للنظام او الشبكة من غير قصد وهذا يعتبر نقطة ضعف

Improperly configured accounts-

إعطاء صلاحيات او أذونات أكثر مما يحتاجه اصحاب الحسابات او غير مناسبة للحسابات

- vulnerable business processes

عمليات الأعمال الغير محصنه وهي الأعمال التجارية للشركات قد تكون نقطة ضعف اذا لم تكن محصنه ضد الهجمات والاختراقات

- Weak cipher suites and implementations

ليست كل خوارزميات التشفير قويه الكثير من الخوارزميات القديمة ضعيفه مما يجعلها نقطة ضعف

- Memory leak

اي برنامج تقوم بتحميله يأخذ مساحة في الذاكرة وعندنا يتم إغلاق البرنامج يفشل البرنامج في تحرير مساحة الذاكرة التي تم أخذها مسبقاً عندما كان قيد التشغيل وبذلك يأخذ مساحة ويسبب نقطة ضعف.

- Pointer dereference

نشاط برمجي لإدخال البرنامج قيمة مخزنه في الذاكرة على اساس عنوانها او المكان المخزنه فيه وفي حال وجود مرجع غير صالح يؤدي الى تعطل البرنامج او فتح ثغره واستغلالها بهجمات Buffer overflows

- System sprawl / undocumented assets

يوجد في الشركات عدد كبير من السيرفرات وممكن ان يكون هنالك سيرفر منسي بسبب صعوبة حصرها وتوثيقها مما قد يسبب نقطة ضعف.

- Architecture / design weaknesses

هي عبارة عن الأخطاء في المفاهيم العامة او مفاهيم التصميم او هيكلة التطبيق،مثل وضع firewalls في مكان غير مناسب وتختص هذه بالبنية التحتية

- New threats / zero day

وهي نقاط الضعف او الثغرات التي لم تكن معروفة مسبقاً ويتم اكتشافها بعد الإختراق

Resource exhaustion

وهي استنفاذ الموارد وهي نقطة ضعف من خلالها يجعل البرنامج يستهلك موارد النظام او الجهاز بدون حد وهنا قد يستغل ذلك من خلال هجوم حجب الخدمة DDOS