CONCEPT

دورة أمن إنترنت الأشياء والأجهزة المدمجة: البرامج الثابتة والبروتوكولات ودورة الحياة الآمنة



دورة أمن إنترنت الأشياء والأجهزة المدمجة: البرامج الثابتة والبروتوكولات ودورة الحياة الآمنة

مقدمة:

أمن إنترنت الأشياء والأجهزة المدمجة، من البرامج الثابتة إلى البروتوكولات ودورة الحياة الآمنة، هو موضوع هذه الدورة الممتدة أسبوع لفرق أمن الأجهزة وأمن المنتجات وهندسة البرامج الثابتة وتصميم الحلول، وتنتهي بإعداد خطة أمن الأجهزة المتصلة. تخرج مستشعرات المدن الذكية وعدادات المرافق والأجهزة الطبية المتصلة في كثير من الأحيان بكلمات مرور افتراضية ومنافذ تصحيح مكشوفة وتحديثات غير موقعة ورسائل بلا مصادقة، فتصبح أساطيل كاملة عرضة للاستيلاء. يعمل المرشحون في تصميم المنتجات المتصلة أو بنائها أو تقييمها، وتقدم الدورة في مختبر عملي على لوحات تطوير وصور برامج ثابتة ووسطاء اختبار. وتقدم كور كونسبت هذه الدورة في أمن إنترنت الأشياء والأجهزة المدمجة.

أهداف الدورة:

- بناء نموذج تهديدات للجهاز يحدد نقاط دخول المهاجم عبر الواجهات المادية والبرامج الثابتة والروابط اللاسلكية والخدمات السحابية الخلفية
- تحديد جذر ثقة مادي وسلسلة إقلاع آمن تتحقق من كل مرحلة في البرامج الثابتة قبل تنفيذها
- استخراج صور البرامج الثابتة وتحليلها لكشف الأسرار المكتوبة داخل الشيفرة والمكونات المتقادمة والإعدادات الافتراضية غير الآمنة
- تقوية الاتصال عبر MQTT وCoAP وBLE بالمصادقة المتبادلة وضبط صلاحيات المواضيع وحماية عملية الاقتران
- تصميم تزويد هوية الأجهزة بشهادات X.509 وعملية تحديث عن بعد موقعة ومحمية من الرجوع إلى إصدارات أقدم
- إعداد خطة أمن الأجهزة المتصلة مع قواعد قياس الأسطول عن بعد والإفصاح عن الثغرات وإخراج الأجهزة من الخدمة في نهاية عمرها

الفئة المستهدفة:

- وظائف أمن الأجهزة والمنتجات المسؤولة عن البنية الأمنية للمنتجات المتصلة
- وظائف هندسة البرامج الثابتة والعتاد التي تبني المستشعرات والبوابات والعدادات ووحدات التحكم في الأجهزة الطبية
- وظائف الاختبار الأمني التي تقيم الأجهزة المتصلة قبل شرائها أو إطلاقها
- وظائف تصميم الحلول التي تربط أساطيل الأجهزة بالوسطاء والخدمات السحابية وخوادم التحديث
- وظائف التقنية في المدن الذكية والمرافق والرعاية الصحية التي تشغل أساطيل كبيرة من الأجهزة الميدانية

محاور الدورة:

اليوم 1: سطح الهجوم على الأجهزة المتصلة ونمذجة التهديدات

- ربط ثغرات OWASP IoT Top 10 قائمة أبرز مخاطر إنترنت الأشياء بالأجهزة الميدانية
- نمذجة التهديدات بطريقة STRIDE لمسارات المستشعر والبوابة والسحابة
- بناء شجرة الهجوم لسيناريوهات الاستيلاء على العدادات الذكية
- مخطط تدفق بيانات الجهاز مع تحديد حدود الثقة
- مراجعة الوضع الأمني الحالي لأسطول أجهزة قيد التشغيل

اليوم 2: خطوط الأساس الأمنية للأجهزة وجذر الثقة والإقلاع الآمن

- خط الأساس لقدرات الأمن السيبراني للجهاز في التعريف والتحديث
- متطلبات المكونات في IEC 62443-4-2 معيار أمن مكونات أنظمة الأتمتة للأجهزة المدمجة
- مستويات التحقق في OWASP ISVS معيار التحقق من أمن إنترنت الأشياء ضمن متطلبات المنتج
- جذر الثقة المادي باستخدام العناصر الآمنة ووحدات TPM
- سلسلة الإقلاع الآمن بمراحل محمل إقلاع موقعة وصمامات إلكترونية

اليوم 3: استخراج البرامج الثابتة وتحليل الملفات التنفيذية والواجهات المادية

- مراحل OWASP FSTM منهجية اختبار أمن البرامج الثابتة للحصول على البرامج الثابتة وتحليلها
- اكتشاف منافذ التصحيح UART وJTAG وSWD وإغلاقها
- استخراج نظام الملفات بأداة Binwalk والبحث عن بيانات الدخول المكتوبة داخل الشيفرة
- إعداد قائمة مكونات البرمجيات SBOM ومطابقة المكونات المتقادمة بالثغرات المعروفة
- تمرين محاكاة واستغلال البرامج الثابتة المعرضة للثغرات في IoTGoat

اليوم 4: ثغرات البروتوكولات وهوية الأجهزة والتحديثات الموقعة عن بعد

- مصادقة وسيط MQTT وقوائم صلاحيات المواضيع وإساءة استخدام مهلة البقاء
- بروتوكول CoAP عبر DTLS بالمفاتيح المشتركة مسبقا والشهادات
- أوضاع الاقتران في BLE والتنصت السلبي وهجمات إعادة الإرسال
- تزويد شهادات X.509 للأجهزة عند التصنيع وتدويرها
- حزم التحديث الموقعة عن بعد مع الحماية من الرجوع والتخفيض

اليوم 5: مختبر على أسطول حالة وإعداد خطة أمن الأجهزة المتصلة

- إحاطة أسطول الحالة لأعمدة الإنارة الذكية والعدادات ومضخات التسريب
- نتائج فجوات نموذج التهديدات والإقلاع الآمن لأجهزة الحالة
- قواعد قياس الأسطول عن بعد لكشف الأجهزة المستنسخة أو المخترقة
- سياسة الإفصاح المنسق عن الثغرات وإخراج الأجهزة من الخدمة
- استكمال خطة أمن الأجهزة المتصلة ومراجعتها بين المشاركين

المهارات التي ستكتسبها:

- نمذجة تهديدات الأجهزة
- تصميم الإقلاع الآمن
- تحليل البرامج الثابتة
- إغلاق واجهات التصحيح
- تقوية بروتوكولات إنترنت الأشياء
- إدارة شهادات الأجهزة
- ضمان سلامة التحديثات عن بعد
- كشف السلوك الشاذ في الأساطيل

لماذا تحضر هذه الدورة:

- تسليم خطة أمن الأجهزة المتصلة إلى مسؤول أمن المنتجات ومدير تشغيل الأسطول لعائلة أجهزة محددة
- الحسم في إطلاق جهاز أو شرائه بعد فحص سلسلة الإقلاع ومنافذ التصحيح وتوقيع التحديثات
- تفادي الاستيلاء على الأسطول واستنساخ الأجهزة وتعطلها الناتج عن كلمات المرور الافتراضية والتحديثات غير الموقعة
- توعية فرق الهندسة والمشتريات بقائمة مراجعة البرامج الثابتة وخط أساس لتقوية البروتوكولات

الخاتمة:

بعد العودة إلى العمل يسلم المشارك خطة أمن الأجهزة المتصلة إلى مسؤول أمن المنتجات ومدير تشغيل الأسطول لعائلة أجهزة واحدة في خدمات المدن الذكية أو المرافق أو الرعاية الصحية. وتعتمد الإدارة على الخطة في تحديد بوابات الإطلاق أو الشراء التي يجب أن يجتازها الجهاز، والشهادات ومفاتيح توقيع التحديثات التي تحتاج إلى حماية أقوى، وقواعد القياس عن بعد التي تكشف الجهاز المستنسخ أو المخترق. وبعد أول إطلاق أو حملة تحديث وفق الخطة تراجع الوحدة نتائج البرامج الثابتة المغلقة، والأجهزة التي ما زالت بلا هوية خاصة بكل جهاز، والتنبيهات مقارنة بالحوادث المؤكدة.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة أمن إنترنت الأشياء والأجهزة المدمجة؟

ينبغي أن يعمل المشارك فعلا على المنتجات المتصلة أو أمنها، وأن يقرأ ملفات التقاط حركة الشبكة ويستخدم سطر أوامر Linux. وتفيد معرفة أساسية ب TLS وشهادات المفتاح العام. ولا تفترض الدورة خبرة سابقة في الهندسة العكسية للبرامج الثابتة، ويفيد وصف عائلة أجهزة يدعمها المشارك في ربط المختبر بعمله.

بم تختلف دورة أمن إنترنت الأشياء والأجهزة المدمجة عن دورات استراتيجية إنترنت الأشياء للأعمال أو برمجة الأنظمة المدمجة؟

تركز هذه الدورة على مهاجمة الجهاز نفسه وحمايته: سلسلة الإقلاع والبرامج الثابتة ومنافذ التصحيح والبروتوكولات اللاسلكية وبروتوكولات المراسلة والهوية والتحديثات. أما دورات الأعمال فتخطط حالات الاستخدام والمشاريع التجريبية، ودورات البرمجة تعلم كتابة المشغلات والمهام الآنية دون تأمينها.

لماذا تكتسب التحديثات الموقعة عن بعد أهمية في أمن إنترنت الأشياء والأجهزة المدمجة؟

تبقى الأجهزة الميدانية في الخدمة سنوات طويلة وتظهر ثغرات جديدة بعد إطلاقها. وتتيح التحديثات الموقعة والمحمية من الرجوع إصلاحها عن بعد، وتمنع المهاجم من تثبيت برامج ثابتة معدلة أو قديمة معرضة للثغرات قد تقود إلى الاستيلاء على أسطول كامل.

ماذا يعود به المشارك من دورة أمن إنترنت الأشياء والأجهزة المدمجة؟

يعود المشارك بخطة أمن الأجهزة المتصلة تضم نموذج تهديدات، وتصميما لجذر الثقة والإقلاع الآمن، ونتائج مراجعة البرامج الثابتة، وإعدادات تقوية البروتوكولات، وتزويد الشهادات، وعملية توقيع التحديثات، وقواعد قياس الأسطول عن بعد، قابلة للتكييف مع عائلة أجهزة في مؤسسته.