Kaspersky Akıllı Teknolojiler ve IoT Güvenlik Değerlendirmesi

Gömülü sistemler gitgide daha karmaşık hale geliyor. Sektör; özelleştirilmiş mikro kontrolör temelli bileşenlerden, onlarca farklı protokol aracılığıyla birbiriyle iletişim kuran gerçek zamanlı ya da Linux tabanlı işletim sistemlerine sahip üçüncü parti SoC platformlarına kurulu, bağlantılı karmaşık çözümlere kadar çok büyük aşamalar kaydetti. Bu türde hızlı bir gelişim, muazzam bir çok yönlülüğü de beraberinde getirir, fakat bunun da bir bedeli vardır: Yaygın bilgi işlem platformlarının gömülü sistemlerde kullanılmaya başlanması, kendine has tehditleri de beraberinde getirmiştir.

Kaspersky Lab, ürünlerinin güvenliğini artırmak ve gelişmiş tehditlere karşı önleyici bir yaklaşım benimsemek isteyen gömülü sistem üreticilerine bir dizi proaktif güvenlik değerlendirmesi hizmeti sunar.

Aşağıdaki potansiyel risk senaryoları tanımlanabilir:

- Son kullanıcılara yönelik arayüzlerden (JTAG, SWD, UART, vb.) hata ayıklama
- Bellek dökümü ve bunu izleyen hassas bilgi ifşası olasılığı
- Ele geçirilen cihazın bileşenleri arasında aktarılan bilgileri arasında hassas bilgilerin olma olasılığı
- Şifreleme planlarının ve algoritmalarının yanlış uygulanması
- Cihazın normal işleyişini engelleyebilecek şekilde üretici yazılımı değişikliği olasılığı
- Sistem yönetimi ve bilgi alışverişi için güvenli olmayan ağ protokollerinin kullanılması
- Kimlik doğrulama ve ayrıcalık ayrımı gibi güvenlik mekanizmalarının yanlış uygulanması
- Arabellek aşımı, aritmetik taşma/yetersizlik (integer overflow/underflow) gibi yaygın görülen gömülü yazılım güvenlik açıkları
- Sabit kodlu kimlik bilgileri, belgelenmemiş kimlik doğrulama atlatma ve ayrıcalık yükseltme mekanizmalarının varlığı.

Gömülü Cihaz Güvenlik Değerlendirmesi

Gömülü cihazların donanım ve yazılım bileşenlerinin kapsamlı güvenlik düzeyi değerlendirmesi. Amaç, suçlular tarafından platformun normal işleyişine zarar vermek için kullanılabilecek potansiyel güvenlik açıklarını, yanlış yapılandırmaları ve tasarım sorunlarını belirlemektir.

Bu hizmetle aşağıdaki türde eylemler yürütülebilir (sistem türüne ve verilen erişim düzeyine bağlı olarak):

- İşletme mantığına ve kullanım gerekliliklerine göre tehdit modelleme
- Güvenlik açığı bulmaya yönelik araştırmalar dahil güvenlik açıklarının manuel ve otomatik olarak belirlenmesi
- Statik, dinamik ve interaktif yaklaşımlar kullanılarak üretici yazılımı ve uygulama kaynak kodu analizi
- Altyapıdaki iletişim protokollerinin ve mevcut güvenlik kontrollerinin güvenlik değerlendirmesi
- Mobil ve kablosuz ağlar dahil (2G/3G/4G, Wi-Fi, Bluetooth, ZigBee, Z-Wave, NFC, vb.) telsiz kanalları güvenliği değerlendirmesi
- İşletim sistemleri ve uygulama bileşenleri için yapılandırma analizi
- Uygulanan güvenlik önlemlerinin değerlendirilmesi
- Ortaya çıkan güvenlik açıklarının kötüye kullanımı ve saldırı tatbikatı
- Bulgular, öneriler ve farklı türdeki tehdit olasılıklarına dair sonuçlar hakkında detaylı bilgi içeren teknik rapor hazırlanması.

Uzmanlarımız sıfır gün güvenlik açığı tespit ettiği takdirde, yazılım üreticilerine tavsiye raporu hazırlar ve aynı zamanda sorumluluk gereği katı bir açıklama politikası izler. Üretici bir güvenlik güncellemesi yayınlayana kadar, keşfedilen güvenlik açıklarıyla ilgili etkileri hafifletecek öneriler de geliştiririz.

Aşağıdaki türde güvenlik açıkları tespit edilebilir:

- Çok faktörlü doğrulama dahil, doğrulama ve yetkilendirme kusurları
- Giriş geçerlik denetimi (aşımlar, bellek sızıntıları vb.)
- Kod enjeksiyonu (SQL enjeksiyonu, işletim sistemi komutları vb.)
- İşlevleri kötüye kullanmaya veya dolandırıcılığa yol açan mantıksal güvenlik açıkları
- Müşteri tarafı güvenlik açıkları (siteler arası komut çalıştırma, siteler arası istek sahteciliği vb.)
- Şifreleme zayıflıkları (plan, uygulama vb.)
- Müşteri tarafı iletişimlerinde güvenlik açıkları
- ve daha fazlası...

Uygulama Güvenliği Değerlendirmesi, Web Uygulaması Güvenliği Değerlendirmesi, Mobil Uygulama Güvenliği Değerlendirmesi

Bu değerlendirmeler, gömülü sistemlerin işlemlerini kontrol etmek ve izlemek için kullanılan uygulamaların ayrıntılı güvenlik analizini içerir. Uygulamanın kaynak kodunun ve mimarisinin statik ve dinamik analizleri buna dahildir. Kaspersky Lab uzmanları, izinsiz giriş yapan kişinin kimlik doğrulama ve yetkilendirme prosedürlerini atlatmasına, ayrıcalıklarını yükseltmesine ya da güvenlik kontrollerinden veya dolandırıcılık tespitinden kaçmasına fırsat verebilecek tüm güvenlik açıklarını bulur.

Uygulama Güvenlik Değerlendirmesi, (hem otomatik hem manuel yaklaşımları kullanarak) şunlara yol açabilecek güvenlik açıklarını tespit etmeyi amaçlar:

- Uygulamanın kontrolünün ele geçirilmesi
- Uygulamanın müşterilerine karşı saldırılar
- Uygulamanın tamamının ya da bir kısmının (bireysel kullanıcıların erişimi engellenerek) hizmetinin engellenmesi
- Uygulamadan önemli bilgilerin elde edilmesi
- Veri bütünlüğünün etkilenmesi.

Analiz sırasında uzmanlarımız yalnızca eski yazılım sürümlerindeki yapılandırma hatalarını ve güvenlik açıklarını bulmakla kalmaz, uygulamanın gerçekleştirdiği işlemlerin arkasındaki mantığı derinlemesine analiz eder, güvenlik mekanizmalarının varlığını ve niteliğini değerlendirir ve yeni güvenlik açıklarını tespit etmeye yönelik güvenlik araştırması yürütür. Bir saldırının etkilerini göstermek ve bulguları doğrulamak için istek üzerine saldırı otomasyonuna yönelik özel araçlar geliştirilebilir.

Analizlerimiz, aşağıdaki türde güvenlik açıklarını tanımlar:

- Savunmasız ağ mimarisi, yetersiz ağ koruması
- Ağ trafiğinin engellenmesine ve yeniden yönlendirilmesine neden olabilecek güvenlik açıkları
- Yetersiz kimlik doğrulama ve yetkilendirme
- Zayıf kullanıcı kimlik bilgileri
- Aşırı kullanıcı ayrıcalığı dahil yapılandırma hataları
- Uygulama kodlarındaki hatalardan kaynaklanan güvenlik açıkları
- Son güvenlik güncellemelerine sahip olmayan eski donanımların ve yazılım sürümlerinin kullanılmasından kaynaklanan güvenlik açıkları
- Bilgilerin ifşa edilmesi

Sızma Testi

Sızma Testi, kritik önem taşıyan sistemlerde mümkün olan en yüksek ayrıcalığı elde etmek için gereken güvenlik kontrollerini atlatma girişimlerini test etmek dahil dışarıdan ve içeriden izinsiz girenlerin gömülü sistemleri kullanmasına olanak sağlayabilecek güvenlik kusurlarını tespit etmek üzere BT altyapısını analiz etmeyi içerir.

İhtiyaçlarınıza ve sistem özelliklerinize bağlı olarak, çeşitli BT altyapı güvenlik değerlendirme hizmetlerinden birini seçebilir veya bunları bir arada kullanabilirsiniz:

- **Dışarıdan sızma testi**: sisteminiz hakkında herhangi bir ön bilgi sahibi olmadan internetten gerçekleştirilen güvenlik değerlendirmesi.
- **İçeriden sızma testi**: örneğin ofisinize yalnızca fiziksel erişimi olan bir ziyaretçi ya da belirli sistemlere kısıtlı erişimi olan bir yüklenici gibi şirket içindeki bir saldırgan adına gerçekleştirilen güvenlik değerlendirmesi.
- **Kablosuz ağ güvenliği değerlendirmesi**: Uzmanlarımız şirketinizi ziyaret ederek Wi-Fi güvenlik kontrollerinizi analiz eder.

Güvenlik Değerlendirmesi Raporu

Güvenlik değerlendirmesi tamamlandıktan sonra müşterilere aşağıdaki ayrıntılı teknik bilgileri içeren bir rapor sunulur:

- Değerlendirme kapsamındaki sistemlerin mevcut güvenlik seviyesine dair üst düzey sonuçlar.
- Hizmet metodolojisinin ve sürecin açıklanması.

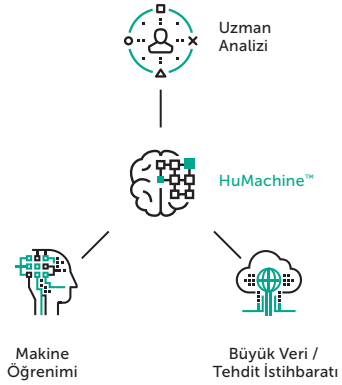
- Önem düzeyleri, açıklardan yararlanmanın karmaşıklığı, zarar görebilecek sistemler üzerindeki olası etkileri ve (mümkün olduğu takdirde) mevcut güvenlik açıklarına dair kanıtlar dahil tespit edilen güvenlik açıklarının ayrıntılı açıklaması.
- Yapılandırma değişiklikleri, güncellemeler, kaynak kodları değiştirme ya da güvenlik açıklarının ortadan kaldırılması mümkün değilse telafi edici kontrollerin uygulanması dahil güvenlik açıklarını ortadan kaldırmaya yönelik tavsiyeler.

Kaspersky Lab Hakkında

Holding şirketi Birleşik Krallık'ta tescilli olan Kaspersky Lab, dünya genelinde yaklaşık 200 ülke ve bölgede faaliyet göstermekte ve dünya çapında 400 milyondan fazla kullanıcı için koruma sağlamaktadır. Kaspersky Lab, dünyada uç nokta koruma çözümü üreten en büyük özel şirkettir. Uç nokta kullanıcıları için güvenlik çözümleri üreten en büyük dört şirket arasında yer almaktayız. Kaspersky Lab, 20 yılı aşkın süredir BT güvenliğinde yenilikçi bir şirket olarak büyük şirketlere, küçük ve orta ölçekli işletmelere ve tüketicilere yönelik etkili dijital güvenlik çözümleri sunmaktadır.

En değerli varlığımız, 20 yılı aşkın süredir BT tehditleriyle savaşırken edindiğimiz, güvenlik açıkları ve kötü amaçlı yazılım araştırmaları, tehlikeli olma potansiyeli taşıyan uygulamalarla mücadele, trafik filtreleri gibi alanlardaki uzmanlığımızdır. Bu uzmanlık, yeni saldırı türlerine karşı en güvenilir korumayı müşterilerimize sağlarken rekabet açısından bir adım önde olmamıza yardımcı olur.

Daha fazla bilgi için: www.kaspersky.com.tr



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliği Haberleri: **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr