Kod Kalitesi Bulguları Hakkında Bir Bilgilendirme

Tespit Edilen Açıklıklar başlığında bahsedilen ve MITRE'nin uluslararası açıklık veri tabanından (Common Weakness Enumeration veri tabanından) referans verilerek sunulan bazı girdiler bir "kod kalitesi" kaydı olabilirler. Ancak bu durum bu türden bulguları önemsiz kılmamaktadır. Bu türden kayıtların Uluslararası açıklık veri tabanında yer alması güvenliğe dokunan bir yanının olduğunu göstermektedir. Şöyle ki uygulamalardaki kod kalitesi ve güvenliği arasında şöyle bir ilişki vardır:

"Kötü kod kalitesi beklenmeyen davranışlara neden olur. Kullanıcı perspektifinden kullanım sorunları yaşatır. Saldırgan perspektifinden sistemi beklenmeyen yollarla denetlemeye bir fırsat olur." -

https://vulncat.fortify.com/en/detail?id=desc.structural.java.dead_code_expression_is_always_false#Java%2fJSP

"*Kod kalitesi yüksek olan uygulamalar daha az hatalı (bug'lı) ve daha az güvenlik açıklıklı eğilimi göstermektedirler*." - Chat GPT

"*Kod kalitesi bir kuruluşu kullanıcı deneyiminin kalitesinden bir uygulamanın **güvenliğine** kadar çeşitli şekillerde etkiler. Kod kalitesi geliştiriciler için çok önemlidir, çünkü kötü yazılmış kod teknik desteğe ve **güvenlik sorunlarına** yol açabilir. Kodun kalitesi bir uygulamanın ne kadar **güvenli** olduğu üzerinde doğrudan bir etkiye sahip olabilir..." -* *https://snyk.io/learn/code-quality/*

"*Kod kalitesi problemleri kendi başına bir güvenlik açıklığı değildirler, fakat güvenlik açıklıklarına yol açmaktadırlar.*" - *https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality*

" *CWE'lerin birçoğu - örneğin Buffer Overflow ve Girdi Denetleme Eksikliği, v.b.'leri - kötü kod kalitesi ve geliştirme pratikleri ile ilişkilendirilir. Kod kalitesini arttırma bazı yazılım **güvenlik açıklıklarını** kapamak için gerekli bir koşuldur. Kötü kod kalitesindeki bir kod parçası ufak dahi olsa zararlı hacker'lar tarafından sömürülebilir güvenlik açıklıklarının doğmasına sebep olabilir. Güvenlik bu nedenle ürünün kalitesine bağımlıdır…Bazı kimseler fonksiyonellik ve güvenilirlik kusurlarının çözümlenmemesi oldukça nadirleşmeye başladı dese de şu kesin ki birçok geliştirici halen kalite standartlarını görmezden geliyor. Burada güvenlik açıklıklarıyla ilişkili kalite standartlarına değinmemize gerek bile yok.*" - *https://fluidattacks.com/blog/code-quality-and-security/*

"*Kod kalitesi güvenlik için gerekli bir koşuldur.*" - *https://www.electronicdesign.com/technologies/embedded-revolution/article/21168142/iar-*

systems-from-code-quality-to-total-security

Kod kalitesi ve kod güvenliği arasındaki bu ilişki nedeniyle uygulamalarda güvenlik açıklığı arayan SAST yazılımları uygulamaların gelecekteki güvenliği için kod kalitesine önem vermektedirler. MITRE'nin CWE'si v.b. uluslararası açıklık veri tabanlarında bu nedenle kod kalitesi kayıtları güvenliğe dokunan bir kayıt olarak yer almaktadır. Uygulama geliştirirken geliştiriciler prensip olarak kod kalitesi kayıtlarının sunduğu ilkeleri takip etmelidirler. Bu ilkelerle hareket edilirse yarının uygulaması daha güvenli olacaktır. Bu ilkeler takip edilmezse yarının uygulamasında güvenlik sorunları daha çok yaşanacaktır. Sonuç olarak kod kalitesi yüksek olan uygulamalar gelecekte daha güvenlidirler. Bu nedenle yarının uygulamasını daha güvenli tutmak için şimdiden kod kalitesine ehemmiyet vermek gerekir. Kod kalitesini yüksek tutmak geleceğe güvenlik anlamında yatırımdır.