Güvenlik Açığı Tespiti

Güvenlik açıkları, tehdit aktörlerinin bu sistemlere yetkisiz erişim elde etmek için istismar edebileceği bilgisayar sistemlerindeki güvenlik kusurlarıdır. İstismardan sonra, kötü amaçlı yazılımlar ve tehdit aktörleri uzaktan kod yürütme, veri sızdırma ve diğer kötü amaçlı faaliyetleri gerçekleştirebilir. Bu nedenle, kuruluşların kötü aktörler istismar etmeden önce ağlarındaki güvenlik açıklarını derhal tespit eden stratejilere veya güvenlik çözümlerine sahip olması gerekir. Bir ağdaki güvenlik açıklarının derhal tespit edilmesi ve düzeltilmesi, genel güvenlik duruşunun güçlendirilmesine yardımcı olur.

Wazuh Vulnerability Detection modülü, kullanıcıların izlenen uç noktalara yüklenen işletim sistemi ve uygulamalardaki güvenlik açıklarını keşfetmelerine yardımcı olur. Modül, aşağıdaki güvenlik açığı kaynaklarından birini kullanarak çalışır.

- Siber Tehdit İstihbaratı (CTI) platformumuzdaki Wazuh zafiyet deposu.
- Çevrimdışı yerel güvenlik açıkları deposu.

Güvenlik açığı bilgilerini sağlamak için Canonical, Debian, Red Hat, Arch Linux, Amazon Linux Advisories Security (ALAS), Microsoft ve National Vulnerability Database (NVD) tarafından dizinlenen harici güvenlik açığı kaynaklarından güvenlik açığı verilerini topluyoruz. Çözümün en son CVE'leri kontrol etmesini sağlayarak bu bilgileri güncel tutuyoruz.

Revision #2
Created 23 December 2024 19:33:39 by Ayşegül Sarıkaya
Updated 31 December 2024 18:00:52 by Ayşegül Sarıkaya