

Proje Referans Makalesi GZFT (SWOT) Analizi

Makale Adı: "OCPPStorm: A Comprehensive Fuzzing Tool for OCPP Implementations"

Analiz Tarihi: 02.11.2025

GÜÇLÜ YÖNLER (Strengths)

- Pratik ve Somut Çıktı:** Araştırma, sadece teorik bir analiz sunmakla kalmayıp, "OCPPStorm" adında çalışan, pratik bir test aracı (fuzzing tool) ortaya koymaktadır.
- Kanıtlanmış Etkinlik:** Araç, iki farklı açık kaynaklı OCPP sistemi üzerinde kapsamlı bir şekilde test edilmiş ve etkinliği kanıtlanmıştır.
- Ciddi Zafiyet Tespiti:** Araştırma, sadece küçük hataları değil, **5'i onaylanmış CVE** (Bilinen Güvenlik Açıkları ve Maruziyetler) ve 7'si incelemede olan **kritik güvenlik açıkları** bulmuştur.
- Sistematik Yaklaşım:** Makale, OCPP implementasyonlarını test etmek için "sistematik bir yaklaşım" tasarlamaya odaklanmıştır.
- Proaktif Güvenlik:** Araştırma, zafiyetleri proaktif (saldırı öncesi) olarak tespit etmeye yönelik bir "proaktif güvenlik tedbiri" sunmaktadır.

ZAYIF YÖNLER (Weaknesses)

- Sınırlı Test Kapsamı:** Makaledeki testler, sadece **iki açık kaynaklı OCPP sistemi** üzerinde gerçekleştirilmiştir. Bu, bulguların piyasadaki tüm kapalı kaynaklı (ticari) sistemler için genellenebilirliğini sınırlar.
- Odak Alanı Sınırlılığı:** Fuzzing tekniği, doğası gereği öncelikle "mesaj yönetimindeki hataları" (errors in the message management) bulmaya odaklanır. Daha karmaşık iş mantığı (business logic) zafiyetlerini tespit etmede yetersiz kalabilir.
- Protokol Sürümü Bağımlılığı:** Makale, test ettiği sistemlerin spesifik OCPP sürümlerine odaklanmış olabilir. Protokolün evrimleştiği göz önüne alındığında, aracın OCPP 2.0.1 gibi daha yeni sürümlerdeki etkinliği belirsizdir.

FIRSATLAR (Opportunities)

- Açık Kaynak Potansiyeli:** Makale, "**OCPPStorm kod tabanının açık kaynak olarak yayınlanacağını**" belirtmektedir. Bu, tüm EV şarj sektörü geliştiricilerinin

ve güvenlik arařtırmacılarının bu aracı ücretsiz olarak kullanıp geliřtirebilmesi için büyük bir fırsattır.

- **Endüstri Standardı Olma:** Sunulan "sistematik yaklaşım", EV řarj istasyonu üreticileri için bir endüstri standardı güvenlik testi (sağlamlık testi) haline gelebilir.
- **Geniřleme Potansiyeli:** Araç, sadece iki sistemde deęil, piyasadaki tüm farklı OCPP implementasyonlarını test etmek için genişletilebilir.
- **Deęerli Bilgi Sağlama:** Arařtırma, geliřtiricilere "potansiyel zayıflıkları belirleme ve ele alma konusunda deęerli bilgiler" sunar.

TEHDİTLER (Threats)

- **Çift Yönlü Kullanım (Dual-Use) Riski:** Açık kaynak olarak yayınlanacak olan OCPPStorm aracı, sadece savunma amaçlı deęil, aynı zamanda **kötü niyetli saldırganlar** tarafından da kullanılabilir. Saldırganlar, bu aracı kullanarak henüz yamalanmamış sistemlerdeki zafiyetleri hızla bulup istismar edebilir.
- **Saldırı Evrimi:** Güvenlik topluluęu bu tür fuzzing araçlarına odaklandıkça, saldırganlar fuzzing'in tespit edemedięi daha karmařık mantık saldırılarına yönelebilir.
- **Protokol Deęiřiklikleri:** OCPP protokolü sürekli evrimleřtikçe, fuzzer aracının sürekli olarak güncellenmesi gerekir, aksi takdirde yeni sürümlerdeki zafiyetleri gözden kaçırabilir.