Kazlıçeşme Mah.245.Sok. Bina No:5 Kat:7 Ofis R-701 Zeytinburnu / ISTANBUL
0212 232 77 55
www.evrim.com

EVRİM YAZILIM BİLGİ TEKNOLOJİLERİ VE GÜVENLİK DEPARTMANI

SİBER GÜVENLİK FAALİYET RAPORU Haziran 2024

Kazlıçeşme Mah.245.Sok. Bina No:5 Kat:7 Ofis R-701 Zeytinburnu / ISTANBUL
0212 232 77 55
www.evrim.com

İçindekiler:

Kazlıçeşme Mah.245.Sok. Bina No:5 Kat:7 Ofis R-701 Zeytinburnu / ISTANBUL
0212 232 77 55
www.evrim.com

1- Yönetici Özeti

Evrim Yazılım olarak daha önce yayınladığımız siber güvenlik faaliyet raporunu yılda üç kere Güvenlik ve penetrasyon testlerimizin ardından sizlerle paylaşacağız. Bu rapor bu anlamda yayınlanan ilk güvenlik sonuç raporudur. Bağımsız ve denetim yetkisi olan Bilishim Siber Güvenlik firması tarafından bu testler gerçekleştirilmişti.

Sistemlerimizde anlık izleme yapan ve remediation sürecinde danışmanlık yapan ADEO firmasından başka bir ekibin dışarından bu testleri yapmasını istedik. Bu durum penetrasyon testlerinin tarafsız ve önyargısız yapılmasını garantiye almak için uygulanan bir yöntemdir. Sızma testi ile white hacker faaliyetlerini yürütmeye başladığında eş zamanlı olarak XDR sistemlerinin bu faaliyetleri yakaladığını böylece test etmiş olduk.

Memnuniyetle gördük ki elde ettiğimiz sonuçların hem iç süreçlerimizde hem müşterilerimiz ile paylaştığımız uygulamalarımızda kritik seviyede bir bulguya rastlanmamıştır.

Sızma testi kapsamında Evrim altyapısı ve sunucularının çalışmasını etkileyecek araçlar kurum yetkililerinin bilgisi olmadan kullanılmamış, hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Internet üzerinden gerçekleştirilen testler, sistemler hakkında herhangi bir bilgisi olmayan personel tarafından gerçekleştirilmiştir.

Test ile sunucular üzerinde bulunabilecek muhtemel güvenlik açıklıklarının kötü niyetli saldırganlardan önce ortaya çıkartılması ve önlem alınması amaçlanmaktadır.

Rapor; bulunan her güvenlik açığının risk derecesini, açık hakkında açıklamaları, açığın nasıl kötüye kullanılabileceğini özetlemektedir. Evrim Yazılım uzman personeli ile her bir madde ile ilgili detaylı yorumlar ile tartışılmış ve eğitimler verilmiştir. .

Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamıştır.

Rapor, okuyucunun TCP/IP ve kullanılan teknoloji hakkında temel bilgilere sahip olduğu düşünülerek hazırlanmıştır. Bu sebeple raporlarda kullanılan terimler ile ilgili herhangi bir açıklama yapılmayacaktır.

2- Genel Test Metodolojisi

Sızma testleri; hedef uygulama üzerinde, kötü niyetli kişiler tarafından elde edilebilecek bilgilerin, bulunan güvenlik zafiyetlerinin, bu güvenlik zafiyetlerinin istismarı sonucunda doğabilecek zararların önceden görülmesi ve uygulamanın sahip olduğu güvenlik risklerinin değerlendirilmesi için gerçekleştirilir. Siyah Kutu, Gri Kutu ve Beyaz Kutu testleri olarak üç farklı yönteme sahiptir. Yöntemler arasındaki farklılık, sızma testi personeline sağlanacak bilgilerde ve testlerin yapılacağı saldırı lokasyonundadır. Buna karşın üç yöntem için de sızma testi sırasında izlenen adımlar aynıdır. Bu adımlar;

1. Planlama: Sızma testi öncesinde, Bilishim ve Evrim Yazılım yetkilileri ile yapılan kapsam belirleme çalışmasıdır. Testin gerçekleştirileceği varlıklar, varlıkların özellikleri, bu varlıklara uygulanması gereken saldırı çeşitleri ve bilgi paylaşımı veya acil durum bildirimleri için irtibat bilgileri belirlenir.
2. Bilgi Toplama: Hedef sistem hakkında bilgi edinme çalışmaları gerçekleştirilir. Herkesin kullanıma açık servisler (arama motoru sonuçları, forumlar, sosyal medya hesapları vs.), otomatik araçlar veya manuel işlemlerle, sistemin kullandığı teknolojiler, bileşen versiyonları, servisler, geçerli kullanıcı adları gibi daha sonraki aşamalarda kullanılabilecek bilgiler toplanır.
3. Zafiyet Keşfi: Bilgi Toplama aşamasında edinilen bilgiler ışığında, sistem üzerinde olası zafiyetler tespit edilir. Zafiyet keşfi, otomatik araçların yardımı ve manuel kontroller ile yapılır. Ayrıca, sistem servisleri üzerinde bilinen açıklıkların varlığı farklı kaynaklardan araştırılır.
4. Açıklık İstismarı: Keşfedilen zafiyetin istismarı için gerekli betikler ve veri yükleri toplanır. Gerekli görüldüğü takdirde, bu gereksinimler sızma testi personeli tarafından oluşturulur ve zafiyetin istismar edilmesi sağlanır. Başarılı istismar sonucunda edinilen yeni kaynaklar, sızma testi içerisinde kullanılır.
5. Raporlama: Önceki adımlarda elde edilen sonuçlar toplanır ve ortak bir rapor hazırlanır. Rapor içerisinde, yalnızca istismar sonuçları değil, bilgi toplama ve zafiyet keşfi aşamalarında tespit edilmiş bulgular da paylaşılır.
6. Doğrulama: Kurum yetkilileri, sızma testi raporunda yer alan bulguları risk seviyelerine göre değerlendirmekle ve zafiyetin giderilmesi için belirtilen çözüm önerilerini uygulamakla yükümlüdür. Alınacak tedbirler tamamlandığında, sızma testi personeli, raporda belirtilen bulguların hala geçerli olup olmadığını denetler ve sonuçları kurum yetkililerine teslim etmek için kaydeder.

Planlama adımı sızma testi öncesinde, Raporlama ve Doğrulama adımları sızma testi sonrasında birer kez tekrarlanır. Bilgi Toplama, Zafiyet Keşfi ve Açıklık İstismarı adımları ise test içerisinde birden fazla kez, döngü halinde, sistem üzerindeki her bileşenin testi tamamlanana kadar sürdürülür. Döngü içerisinde edinilen bulgular, nedenleri ve ekran görüntüleri ile birlikte Raporlama adımı için saklanır.

3- Risk Derecelendirme Yöntemi

Sızma testi çalışmalarında bulunan açıklar 5 risk seviyesinde değerlendirilmişlerdir. Bu değerlendirmede, PCI- DSS güvenlik tarama prosedürleri dokümanında1 kullanılan beş seviye risk değerleri kullanılmıştır.

ÖNEM SEVİYESİ	AÇIKLAMA
ACİL	Bu seviyedeki açıklıklar kolaylıkla istismar edilebilir. Saldırganlar genele açık sistemler üzerinden hedef sistemi ele geçirebilir. Bu seviyedeki zafiyetlere örnek olarak, genel erişime açık kurum sistemleri üzerinden dosya ve veri tabanı okuma/yazma erişimi elde edilmesi, uzaktan kod çalıştırma, arka kapıların (backdoor) varlığı ve işletim sistemi üzerinde komut çalıştırma gösterilebilir.
KRİTİK	Bu seviyedeki açıklıklar istismar edilerek sistemlerin ele geçirilmesi ya da yüksek kritiklik seviyesindeki verilerin sızdırılması mümkün olabilir. Bu seviyedeki zafiyetler istismar edilerek sisteme kısıtlı yetkilerle erişim sağlanabilir ya da zafiyet sadece iç ağ üzerinden istismar edilebilir. Bu seviyedeki zafiyetlere örnek olarak dosya ve veri tabanı okuma erişiminin elde edilmesi, kurum kullanıcı bilgileri ve kaynak kodlar gibi hassas verilerin sızdırılması ve olası arka kapılar (backdoor) gösterilebilir.
YÜKSEK	Bu seviyedeki güvenlik açıklıkları hedef sistemdeki önemli yapılandırma bilgilerinin ele geçirilmesine ya da sistemin servis dışı kalmasına (DoS) neden olabilir. Bu seviyedeki zafiyetlere örnek olarak sistemdeki yapılandırma dosyalarının ifşası, dizin gezinimi, servislerin yetkisiz kullanılabilmesi ve servis dışı bırakma (DoS) gösterilebilir.
ORTA	Bu seviyedeki güvenlik açıklıkları saldırganların işlerini kolaylaştıracak yazılım sürümleri gibi bazı bilgilerin açığa çıkmasına neden olabilir. Bu bilgilerin ifşası saldırganların bilinen istismar kodlarını kullanma riskini ortaya çıkarmaktadır.
DÜŞÜK	Literatürdeki en iyi kullanım yöntemlerinin (best practices) izlenmemesinden kaynaklanan ve sistemle ilgili basit bilgilerin açığa çıkmasına sebep olan açıklıklardır.
BİLGİ	Genel olarak saldırganın kuruluş, çalışanlar, uygulamalar ve sistem hakkında bilgi toplayabildiği durumları ifade eder. Mutlaka bir güvenlik açığı anlamına gelmemekle birlikte saldırganın elde ettiği herhangi bir bilginin, daha sonra bir saldırıyı daha doğru bir şekilde kurgulamak ve uygulamak amacıyla kullanılabileceği unutulmamalıdır. Bu nedenle herhangi bir bilgi ifşasının mümkün olduğunca kısıtlaması önerilir. Bununla birlikte bilgi seviyesinde sunulan bulgular; eski versiyon ürün kullanımları, konfigürasyon hataları gibi düşük risk seviyesinin de altındaki güvenlik açıklarını, atak yüzeyinin daraltılmasına yardımcı önerileri ve en iyi kullanım yöntemlerinin (best practices) önerilerini de kapsayabilir.

4. İnceleme ve Analiz Sonuçları

Aşağıda belirtilen servis ve uygulamalar ilişkin doğrulama raporları talep edilmesi halinde kişisel olarak paylaşılacaktır.

cepgumruk.evrimbilgisayar.com
evrimbilgisayar.com
Masaüstü Uygulamaları ve Evrim Gümrük XML servisi
update.evrim.com
vrbprod.evrim.com
webgumruk.evrim.com
haber.evrim.com
*.evrimx.com

Ek-1 Evrim Masaüstü Uygulamaları Servis Erişim Listesi

- **Gümrük sistemine erişim yetkisi (Client ve Server)**

  Gumruk Bakanligindan ilgili TCGB işlemleri igin bakanligin aşagida sagladigi web servisleri araciligi ile, ithalat ve ihracat beyanname tescillerinin alinmasi ve beyanname sorgulama işlemleri gergekleştirilmesi saglanir.

  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/KontrolHizmetiWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/GumrukIdareleriNotlariWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/OzetBeyanWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/TescilWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/HatBildirWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/ETicaretWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/ETicaretSorgulamalarWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/GumrukWS
  https://ws.gtb.gov.tr:8443/EXT/Gumruk/EGE/Provider/AktarmaWS

- **Medos sistemine erişim yetkisi (Client ve Server)**

  Aşagidaki servisler (TIM veya TOBB), ihracat evraklarinin onayi igin beyanname bilgileri ile kendi imza kartlari uzerinden imzalanarak Medos sistemine aktarimi ve onay alinmasi igin kullanilir.

https://medos.tobb.org.tr/services/service02.php
https://istanbul.ebirlik.net/dolasim/services/TimMedos7wsdl

- **Birlik Yapılabilmesi için erişim verilecek ftp adresleri (Client ve Server)**

  Turkiye ihracatgilar Meclisine (TiM) bagli olarak yapilacak Birlik ve Kayit Belgesi işlemleri igin gumruk beyanname bilgileri ile aşagidaki FTP adresleri kullanilarak , Onay ve Odeme işlemleri gergekleştirilir. Sonug olarak, işlemlerin sonrasinda gerekli kayit numaralari ilgili beyanname uzerine işlenmektedir.

  ftp://ftpistanbul.ebirlik.net
  ftp://ftpankara.ebirlik.net

- **Programin Erişecegi web siteleri (Client ve Server)**

Kullanicilarin uygulama igerisinden Evrim Destek Qozum Portali uzerinde yayinlanan makalelere erişmek igin aşagidaki servis kullanilir.

https://destek.evrim.com/portal/tr/kb

Kullanıcıların Evrim Ekosisteminin genelini ilgilendiren tum haber ve duyurulara erişim için kullanilan servis.

https://haber.evrim.com

Evrim Uygulamalarinin Lisans ve Versiyon durumunu sorgulayan, bununla birlikte Medos,E-Fatura ve TPS/Tareks, Sigorta/Polige urunleri igin kontor sayag islevini saglayan servis.

https://lisanskontrol.evrim.com

Evrim Yazilim tarafindan Uygulamalar uzerinde yapilan guncellemeler (.exe, .zip, .txt, .sql uzantili dosyalar) , kullanici kimlik dogrulama altyapisina bagli olan asagidaki servis ile kullanicilar tarafindan gekilmektedir.

https://update.evrim.com

Kazlıçeşme Mah.245.Sok. Bina No:5 Kat:7 Ofis R-701 Zeytinburnu / ISTANBUL
0212 232 77 55
www.evrim.com

Ek-2 Evrim Uygulamaları Web Servis Topolojisi