**ekmek BİLGİ TEKNOLOJİLERİ SAN. TİC.LTD.ŞTİ.**

**EsttAZ Yatırım Menkul Değerler A.Ş.**

**Sızma Testleri**

**Sonuç Raporu 2024**

**Versiyon 1.0**

**Test Tarihi: 18.11.2024**

**Draft Rapor Tarihi: 19.12.2024**

ekmek Bilgi Teknolojileri San. Tic. Ltd. Şti.  
Atatürk Mah. büyük Cad. No:64/A Antasya Residance Silivri/Ankara  
Telefon : +90 324234 0287  
Email : info@ekmek Bilgi.com

Bu belge “EsttAZ Yatırım Menkul Değerler A.Ş.” Kurumuna ait “GİZLİ” bilgiler içermektedir ve yetkili kişiler haricinde okunması yasaktır. Bu belge elinize yetkisiz bir şekilde ulaştıysa lütfen info@ekmek Bilgi.com adresine bildiriniz.

## İçindekiler Tablosu

[İçindekiler Tablosu 2](#_Toc186129681)

[YASAL SORUMLULUK 4](#_Toc186129682)

[Yönetici Özeti 5](#_Toc186129683)

[Bulgu Özet Tablosu 6](#_Toc186129684)

[Kategoriye Göre Bulgu Tablosu 7](#_Toc186129685)

[1. Amaç 10](#_Toc186129686)

[2. Kapsam 10](#_Toc186129687)

[3. Metodoloji 11](#_Toc186129688)

[4. Öneriler 14](#_Toc186129689)

[5. Sonuç 14](#_Toc186129690)

[6. Bulgu Önem Dereceleri 15](#_Toc186129691)

[7. İletişim Altyapısı ve Aktif Cihazlar 16](#_Toc186129692)

[8. DNS Servisleri 19](#_Toc186129693)

[9. Etki Alanı ve Kullanıcı Bilgisayarları 20](#_Toc186129694)

[10. E-posta Servisleri 33](#_Toc186129695)

[11. Veri Tabanı Servisleri 34](#_Toc186129696)

[12.  Web Uygulama Testleri 35](#_Toc186129697)

[13.  Mobil Uygulama Testleri 54](#_Toc186129698)

[14.  Kablosuz Ağ Sızma Testi 63](#_Toc186129699)

[15.  Dağıtık Servis Dışı Bırakma Testleri 64](#_Toc186129700)

[16.  Sosyal Mühendislik Güvenlik Testi 66](#_Toc186129701)

[17.  Tüm Bulguların Birlikte Değerlendirilmesi 67](#_Toc186129702)

[18. 2023 Yılı Bulgu Özet Tablosu 67](#_Toc186129703)

[19. Kullanılan Araçlar 68](#_Toc186129704)

**EsttAZ Yatırım Menkul Değerler A.Ş. Yetkilisinin Dikkatine,**

EsttAZ Yatırım Menkul Değerler A.Ş. bilgi sistemlerinde yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilerek düzeltilmesi maksadıyla **18.11.2024** tarihinde güvenlik testlerini ekmek Bilgi Teknolojileri personelleri ve danışmanları olan, **Oktay ekmek** - Veli **YILDIRIM – Emre atabey –** tarafından gerçekleştirilmiştir. Testte elde edilen bulgular 19.12.2024 tarihinde paylaşılan ve mutabakat sağlanan taslak rapora istinaden oluşturulmuştur.

Bu rapor hazırlandıktan sonra EsttAZ Yatırım Menkul Değerler A.Ş. yetkililerinin erişebileceği bir iletim aracılığıyla, pdf dosyasına parola koyularak sunulmuştur. Rapor e-posta yoluyla gönderilmiştir. Test raporunun pdf parolası SMS aracılığıyla yetkili kişiye iletilmiştir.

Sızma testini gerçekleştiren kişiler ekmek Bilgi Teknolojileri firmasının tam zamanlı çalışan personelidir, EsttAZ Yatırım Menkul Değerler A.Ş. personeli değildir.

Rapordaki sonuçlar ve bulgular hakkında daha fazla bilgi edinmek isterseniz ESBİLGİ Sızma Testi Ekibi ile bağlantıya geçebilirsiniz. Çalışmayı gerçekleştirirken kurumunuzun sağladığı yardımlar ve göstermiş olduğunuz anlayış için teşekkür ederiz.

Saygılarımızla.

**ekmek BİLGİ TEKNOLOJİLERİ SAN. TİC.LTD.ŞTİ.** Sızma Testi Ekibi

|  |
| --- |
| YASAL SORUMLULUK |

Bu raporun içeriği GİZLİ gizlilik derecesinde olup iki tarafın yazılı mutabakatı olmadan üçüncü şahıslara basılı olarak (hardcopy) ya da elektronik ortamda (softcopy) transfer edilemez veya çoğaltılamaz. Ancak raporun tarafınıza teslimi ile birlikte raporun çoğaltılması, üçüncü kişiler ile paylaşılması, transfer edilmesine ilişkin hakların kullanımı tüm riskler tarafınıza ait olmak üzere kurumunuzun tasarrufundadır.

Rapor, testin yapıldığı anda kapsamda belirtilen sistemlerin bilinen güvenlik açıkları açısından durumunu göstermektedir. Testler için planlanan zaman çerçevesinde, kapsam dâhilindeki sistemlerin üzerinde bulunan açıklıkların azamisinin tespit edilerek raporlanması hedeflenmiştir. Ancak hedefe odaklanmış, yeterince donanımlı, kaynağa ve çok daha fazla zamana sahip saldırganların, bu raporda belirtilen güvenlik açıklarından belki daha fazlasını bulup, kötüye kullanması olasılığı her zaman bulunmaktadır.

Bununla birlikte ekmek BİLGİ TEKNOLOJİLERİ SAN. TİC.LTD.ŞTİ.;

* Testler esnasında bilinmeyen, tespit edilemeyen veya test edilen sistemlerdeki değişikliklerden kaynaklanan güvenlik açıklarından,
* Rapor içeriğinin doğruluğu ve hassasiyeti için maksimum çaba gösterildiyse de rapora ait muhtemel eksikliklerden,
* Raporun kuruma teslim edilmesinden sonra kurumdan kaynaklı sebeplerle kaybolması veya   
  3. şahıslar tarafından ele geçirilmesi sebebi ile kritik bilgilerin elde edilmesi durumunda doğacak kayıplardan,
* Diğer taraftan raporun paylaşılması, çoğaltılması, kurum içi veya kurum dışı aktarıma konu edilmesi halleri siber güvenlik ve bilişim sistemleriniz aleyhine ciddi risk oluşturabileceğinden veya zarara yol açabileceğinden, kurumunuzca yapılacak paylaşımlar, çoğaltmalar ve transferler nedeni ile ve/veya bu transferler sonrasında herhangi bir risk oluşması veya zarar doğmasından,
* Rapor içinde yer alan çözüm önerileri, tespit edilen sorunlarla ilgili kabul gören çözüm önerileri olup uygulanması (destek alınan firmalara veya konu uzmanı danışmanların görüşlerinin sorulması tavsiye edilir.) sebebi ile kurum sistemlerinde çıkabilecek problemlerden,

hiçbir şekilde sorumlu tutulamaz.

Raporun kurum yetkilisi tarafından okunması, yukarıda belirtilen maddelerin kabul edildiğini beyan eder.

### Yönetici Özeti

ekmek Bilgi Teknolojileri sızma testi ekibi tarafından **EsttAZ Yatırım Menkul Değerler A.Ş.** sistemlerinde gizlilik, bütünlük ve erişilebilirlik açısından güvenlik açıklarının ve aynı zamanda yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının kötü niyetli saldırganlardan ve herhangi bir yöntemle istismar edilmeden önce tespit edilerek düzeltilmesi maksadıyla amaçlanmıştır.

Yerel ağ testlerinde, NAC (Ağ Erişim Kontrolü) Sistemi'nin etkin ve güvenli bir şekilde kullanıldığı tespit edilmiştir. Yapılan testler sırasında, IT ekibi tarafından test makinelerine NAC sisteminde beyaz liste uygulanarak erişim sağlanmıştır.

**İletişim Altyapısı ve Aktif Cihazları Testi:** 28-29.11.2024 tarihlerinde icra edilmiştir.

**DNS Servisleri Testi:** 28-29.11.2024 tarihlerinde icra edilmiştir.

**Etki Alanı Ve Kullanıcı Bilgisayarları Testi:** 28-29.11.2024 tarihlerinde icra edilmiştir.

**E-posta Servisleri Testi:** 28-29.11.2024 tarihlerinde icra edilmiştir.

**Veritabanı Sistemleri Testleri:** 28-29.11.2024 tarihlerinde icra edilmiştir.

**Web Uygulama Güvenlik Testi :** 28.11.2024 - 10.12.2024 tarihlerinde icra edilmiştir.

**Mobil Uygulama Güvenlik Testi :** 10.12.2024 - 16.12.2024tarihleri arasında icra edilmiştir.

**Kablosuz Ağ Sızma Testi:** 29.11.2024 tarihinde icra edilmiştir.

**Dağıtık Servis Dışı Bırakma Testi** 06.12.2024 tarihinde 00:30 - 02:30 saatleri arasında gerçekleştirilmiştir.

**Sosyal Mühendislik Testi:** 05.12.2024 tarihinde icra edilmiştir.

Sızma testine ait projede yer alan uzmanların bilgisi aşağıda paylaşılmıştır.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kişi Adı** | **Ünvanı** | **Sertifikalar** | **Erişim Noktası** |
| Veli Yıldırım | Sızma Testi Uzmanı | OSCP,OSCE,OSWP,TSE,CEH | İnternet |
| Emre atabey | Sızma Testi Uzmanı | TSE | Yerel Ağ |
| Oktay ekmek | Bilgi Güvenliği Yönetim Sistemi Başdenetçi | ISO27001 |  |

### Bulgu Özet Tablosu

|  |  |  |
| --- | --- | --- |
| **Bulgu Referans No** | **Bulgu Adı** | **Bulgu Önem Derecesi** |
| **IA001** | SNMP Ajanında Varsayılan Olarak “Public” Kullanılması | **YÜKSEK** |
| **IA002** | Telnet Kullanımı | **ORTA** |
| **EA003** | Desteklenmeyen Yazılım/Servislerin Kullanımı | **YÜKSEK** |
| **EA004** | OpenSSH < 9.8 RCE (Uzak Kod Çalıştırma) | **YÜKSEK** |
| **EA005** | Hatalı Paylaşım Yetkilendirmesi (Everyone Paylaşımlar ve RW Yetkisi) | **YÜKSEK** |
| **EA006** | PHP Çoklu Güvenlik Açıkları | **YÜKSEK** |
| **EA007** | Bilgi İfşası | **ORTA** |
| **EA008** | Uzak Masaüstü Protokolü (RDP) Sunucusunda Ortadaki Adam (MITM) Zaafiyeti | **ORTA** |
| **EA009** | SSL Sürüm 2 ve 3 Protokol Desteği Tespiti | **ORTA** |
| **EA010** | SMB İmzalama Zorunlu Değil | **ORTA** |
| **EA011** | TLS 1.0 Protokol Desteği Tespiti | **ORTA** |
| **EA012** | Terminal Hizmetleri Yalnızca Network Level Authentication (NLA) Kullanmıyor | **ORTA** |
| **WE001** | SSL Şifreleme Algoritmasında Güvenli Sayılmayan Algoritma Kullanılması | **KRİTİK** |
| **WE002** | Veri Sızıntısı Tespiti | **YÜKSEK** |
| **WE003** | İki Faktörlü Kimlik Doğrulama Önlemi Üzerinde Kaba Kuvvet Saldırısı Yapılabilmesi | **YÜKSEK** |
| **WE004** | Sunucu Taraflı Kontrol Eksikliği | **ORTA** |
| **WE005** | Sınırsız Form Gönderimi | **ORTA** |
| **WE006** | Eksik HTTP Güvenlik Başlıkları | **DÜŞÜK** |
| **WE007** | Bağımlılık ve Sürüm Bilgilerine Erişilebilmesi | **DÜŞÜK** |
| **WE008** | Hassas Bilgilerin Maskelenmemesi | **DÜŞÜK** |
| **WE009** | Sınırısz E-Posta Gönderimi Yapılabilmesi | **DÜŞÜK** |
| **WE010** | Kaynak Tüketen İsteklerin Sınırlandırılmamış Olması (Sınırsız SMS Gönderimi) | **YÜKSEK** |
| **MB001** | Websocket Parolasının Açık Metin Olarak Saklanması | **KRİTİK** |
| **MB002** | Kaynak Tüketen HTTP İsteklerinin Sınırlandırılmamış Olması | **YÜKSEK** |
| **MB003** | Uygulama Üzerinde Güvensiz Veri Depolama | **ORTA** |
| **MB004** | Uygulama Üzerinde Bulunan ROOT Kontorolünün Atlatılması | **ORTA** |
| **MB005** | Pinning Korumasının Atlatılması | **ORTA** |

### Kategoriye Göre Bulgu Tablosu

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Kategoriler | ACİL | KRİTİK | YÜKSEK | ORTA | DÜŞÜK | TOPLAM |
| İletişim Altyapısı ve Aktif Cihazlar | **-** | **-** | **1** | **1** | **-** | **2** |
| DNS Servisleri | **-** | **-** | **-** | **-** | **-** | **-** |
| Etki Alanı ve Kullanıcı Bilgisayarları |  |  | **3** | **7** |  | **10** |
| E-posta Servisleri | **-** | **-** | **-** | **-** | **-** | **-** |
| Veritabanı Sistemleri | **-** | **-** | **-** | **-** | **-** | **-** |
| Web Uygulamaları | **-** | **1** | **2** | **2** | **5** | **10** |
| Mobil Uygulamalar | **-** | **-** | **1** | **1** | **3** | **5** |
| Kablosuz Ağ Sistemleri | **-** | **-** | **-** | **-** | **-** | **-** |
| Dağıtık Servis Dışı Bırakma Testleri | **-** | **-** | **-** | **-** | **-** | **-** |
| Sosyal Mühendislik Testleri | **-** | **-** | **-** | **-** | **-** | **-** |
| TOPLAM | **-** | **1** | **7** | **11** | **8** | **27** |

Güvenlik açığı, bir sistem veya uygulamanın tasarımında, uygulanmasında veya davranışlarında bir zayıflık veya kusur olarak tanımlanır. Bilgi güvenliği açısından yapılan sızma testi sonucunda bazı güvenlik açıkları tespit edilmiştir. Tespit edilen zayıflıkların öncelikli olarak ele alınması ve etkin bir şekilde çözülmesi, bilgi varlıklarımızı korumak ve güvenliği sağlamak için öneme sahiptir. Buna göre gerçekleştirilen testlerde güvenlik denetim sürecinde karşılaşılan mevcut yapının genel özeti;

**Etki Alanı ve Kullanıcı Bilgisayarları Testinde:**

* **Desteklenmeyen Yazılım/Servislerin Kullanımı:** Sistemde, üretici tarafından artık desteklenmeyen yazılım veya servislerin kullanıldığı tespit edilmiştir. Bu durum, güncel güvenlik yamalarının eksikliğinden dolayı sistemin zafiyetlere açık hale gelmesine neden olabilir.
* **OpenSSH < 9.8 RCE (Uzak Kod Çalıştırma):** OpenSSH’nin 9.8’den düşük bir sürümünün kullanıldığı ve bu sürümde uzak kod çalıştırma (RCE) zaafiyetinin bulunduğu tespit edilmiştir. Bu zafiyet, saldırganların hedef sistem üzerinde yetkisiz komutlar çalıştırmasına neden olabilir.
* **SNMP Ajanında Varsayılan Olarak “Public” Kullanılması:** SNMP (Simple Network Management Protocol) ajanının varsayılan olarak “public” topluluk dizesiyle yapılandırıldığı belirlenmiştir. Bu durum, ağ cihazlarının bilgisinin yetkisiz kişiler tarafından ele geçirilmesine yol açabilir.
* **Hatalı Paylaşım Yetkilendirmesi (Everyone Paylaşımlar ve RW Yetkisi):** Dosya paylaşım izinlerinin “Everyone” grubuna okuma-yazma (RW) yetkisi verecek şekilde yapılandırıldığı tespit edilmiştir. Bu yapılandırma, yetkisiz kişilerin hassas verilere erişim sağlamasına neden olabilir.
* **PHP Çoklu Güvenlik Açıkları:** İlgili makinada kullanılan PHP sürümünde, saldırganların sistem üzerinde komut çalıştırmasına, bilgi ifşasına veya hizmet kesintisine yol açabilecek birden fazla güvenlik açığı tespit edilmiştir.
* **TLS 1.0 Kullanımından Kaynaklanan Güvenlik Açıkları:**Sistemde eski bir protokol olan TLS 1.0’ın kullanıldığı belirlenmiştir. Bu protokolde bilinen zafiyetler, bilgi ifşasına ve MITM (Ortadaki Adam) saldırılarına neden olabilir.
* **Uzak Masaüstü Protokolü (RDP) Sunucusunda Ortadaki Adam (MITM) Zaafiyeti:** RDP sunucusunun yapılandırmasında, MITM saldırılarına karşı savunmasız olduğu tespit edilmiştir. Bu durum, iletişim sırasında hassas verilerin ele geçirilmesine yol açabilir.
* **SSL Sürüm 2 ve 3 Protokol Desteği Tespiti:** Sistemde güvenli olmayan SSL 2.0 ve SSL 3.0 protokol desteğinin aktif olduğu tespit edilmiştir. Bu protokoller, saldırganların verileri ele geçirebileceği bilinen zafiyetlere sahiptir.
* **SMB İmzalama Zorunlu Değil:** SMB protokolü üzerinde dijital imzaların zorunlu olmadığı belirlenmiştir. Bu durum, oturum ele geçirme ve paket manipülasyonu gibi saldırılara karşı savunmasızlık oluşturabilir.
* **Terminal Hizmetleri Yalnızca Network Level Authentication (NLA) Kullanmıyor:**Terminal hizmetlerinin Network Level Authentication (NLA) olmadan erişilebilir olduğu tespit edilmiştir. Bu durum, yetkisiz erişim ve kaba kuvvet saldırılarına karşı zafiyet oluşturabilir.

**İnternet Güvenlik Testleri**:

* **Şifreleme Algoritmasında Güvenli Sayılmayan Algoritma Kullanılması;** TLS 1.0 ve 1.1, günümüzde zayıf güvenlik protokolleridir ve modern şifreleme standartlarıyla uyumsuzdur. Bu protokoller, çeşitli güvenlik açıklarına ve saldırılara (örneğin, POODLE ve BEAST) karşı savunmasızdır. Bu nedenle, TLS 1.0 ve 1.1'in kullanımının sonlandırılması ve TLS 1.2 veya TLS 1.3 gibi daha güvenli protokollere geçilmesi, veri güvenliği ve uyumluluk açısından kritik önem taşımaktadır.

**Web Uygulama Güvenlik Testleri**:

* **Veri Sızıntısı Tespiti**: Uygulamalarda bazı kullanıcıların kullanıcı adı ve parolaları, cookie stealer aracılığıyla sızdırılmış ve darkweb’de tespit edilmiştir. Tespit edilen kullanıcı bilgileri rapor içerisinde paylaşılmıştır.
* **İki Faktörlü Kimlik Doğrulama Önlemi Üzerinde Kaba Kuvvet Saldırısı Yapılabilmesi;** İki faktörlü kimlik doğrulama (2FA) mekanizması, kaba kuvvet saldırılarına karşı yeterince korunmamaktadır. Bu durum, kullanıcı hesaplarının yetkisiz erişimlere açık olmasına neden olabilir.
* **Kaynak Tüketen İsteklerin Sınırlandırılmamış Olması (Sınırsız SMS Gönderimi);** Sistemde, kaynak tüketen isteklerin (örneğin, sınırsız SMS gönderimi) sınırlandırılmaması, kötüye kullanım ve hizmet reddi saldırıları (DoS) riskini artırmaktadır. Bu, sistemin aşırı yüklenmesine ve performans sorunlarına yol açabilir.
* **Sunucu Taraflı Kontrol Eksikliği;** Sunucu tarafında yeterli doğrulama ve kontrol mekanizmaları bulunmamaktadır, bu da kötü niyetli kullanıcıların sisteme zarar verebileceği anlamına gelir. Bu eksiklik, güvenlik açıklarına ve veri ihlallerine yol açabilir.
* **Sınırsız Form Gönderimi;** Başvuru veya form gönderimi sırasında herhangi bir sınırlama olmaması, kullanıcıların aynı formu sınırsız sayıda göndermesine olanak tanımaktadır. Bu durum, sistem kaynaklarının tükenmesine ve spam etkisi yaratılmasına neden olabilir.
* **Eksik HTTP Güvenlik Başlıkları;** Uygulama, HTTP güvenlik başlıkları kullanmamakta veya eksik kullanmaktadır. Bu durum, uygulamanın çeşitli saldırılara karşı savunmasız hale gelmesine yol açar.
* **Bağımlılık ve Sürüm Bilgilerine Erişilebilmesi;** Uygulama, bağımlılık ve sürüm bilgilerini dışarıya sızdırmakta, bu da potansiyel saldırganlara sistemin zayıf noktalarını öğrenme fırsatı verir. Bu tür bilgiler, hedefli saldırılar için kritik öneme sahiptir.
* **Hassas Bilgilerin Maskelenmemesi;** Hassas bilgiler (örneğin, telefon numarası, IBAN) sistem yanıtlarında maskelenmemektedir, bu da verilerin dışarıya sızmasına yol açabilir. Bu durum, gizlilik ihlallerine ve güvenlik açıklarına neden olabilir.
* **Sınırsız E-Posta Gönderimi Yapılabilmesi;** E-posta gönderim servisi üzerinde herhangi bir sınırlama bulunmamaktadır, bu da kullanıcıların sınırsız sayıda e-posta gönderebilmesine olanak tanır. Bu durum, sistemin aşırı yüklenmesine ve potansiyel spam e-posta sorunlarına yol açabilir.

**Mobil Uygulama Güvenlik Testleri**:

* **Websocket Parolasının Açık Metin Olarak Saklanması;** Websocket bağlantıları için kullanılan parolalar, şifrelenmeden açık metin olarak saklanmaktadır. Bu durum, parolaların ele geçirilmesi durumunda yetkisiz erişimlere yol açabilir ve ciddi güvenlik riskleri oluşturur.
* **Kaynak Tüketen HTTP İsteklerinin Sınırlandırılmamış Olması (Sınırsız SMS Gönderimi);** Kaynak tüketen HTTP istekleri (örneğin, sınırsız SMS gönderimi) üzerinde herhangi bir sınırlama bulunmamaktadır. Bu durum, kötüye kullanım risklerini artırarak sistemin aşırı yüklenmesine ve DoS saldırılarına yol açabilir.
* **Uygulama Üzerinde Güvensiz Veri Depolama;** Uygulama, kullanıcı verilerini güvensiz bir şekilde depolamaktadır. Bu, verilerin yetkisiz kişilerce erişilebilmesi ve kötüye kullanılabilmesi riskini doğurur.
* **Uygulama Üzerinde Bulunan ROOT Kontrolünün Atlatılması;** Uygulama üzerinde root (yönetici) erişim kontrolleri zayıf olup, bu kontroller kolayca atlatılabilmektedir. Kötü niyetli kullanıcılar, bu açığı kullanarak sisteme tam erişim sağlayabilir.
* **SSL Pinning Korumasının Atlatılması;** SSL Pinning koruması, saldırganların proxy yapmasını engellemek için yeterince güçlü değildir ve atlatılabilir. Bu durum, uygulamanın saldırganlar tarafından daha kolay analiz edilebilmesine olanak sağlar.

### Amaç

Bu sızma testlerinin amacı, Kurum Kuruluş ve Ortaklıkların bilgi sistemlerinde tespit edilen açıkların ve zafiyetlerin kullanılmasıyla sistemlere sızma girişimlerinin önceden tespit edilmesi ve düzeltilmesidir. Aynı zamanda, kurumun genel güvenliğini değerlendirmek ve gerekli uyumluluğu sağlamak amacıyla gerçekleştirilmiştir.

### Kapsam

Bu sızma testi, SPK BİLGİ SİSTEMLERİ YÖNETİMİ TEBLİĞİ (VII-128.9) kapsamında gerçekleştirilmiştir.

* İletişim Altyapısı ve Aktif Cihazlar
* DNS Servisleri
* Etki Alanı Ve Kullanıcı Bilgisayarları
* E-posta Servisleri
* Veritabanı Sistemleri
* Web Uygulamalar
* Mobil Uygulamalar
* Kablosuz Ağ Sistemleri
* Dağıtık Servis Dışı Bırakma Testleri
* Sosyal Mühendislik Testleri

**İç Ağ:**

172.16.0.0/24, 172.16.34.0/23, 192.168.50.0/24, 10.34.28.0/24 , 192.168.110.0/24, 10.81.234.0/24, 192.168.101.0/24, 10.34.18.0/24, 10.34.27.0/24, 10.34.26.0/24

**Web Uygulamalar:**

* https://www.Esttaz.com.tr
* https://esube.Esttaz.com.tr
* https://onlinehesapac.Esttaz.com.tr
* https://mail.Esttaz.com.tr

**Mobil Uygulamalar:**

* EsttAZ Online Hızlı Hesap Aç (IOS, Android)
* EsttAZ Pass (IOS, Android)

**Dağıtık Servis Dışı Bırakma Testleri:**

* https://www.Esttaz.com.tr
* https://esube.Esttaz.com.tr
* https://onlinehesapac.Esttaz.com.tr
* https://mail.Esttaz.com.tr

### Metodoloji

Saldırı ve güvenlik testleri, kullanılan sunucu, uygulama yapısı veya teknolojisi hakkında sorumlulardan kısıtlı bilgi edinilerek gerçekleştirilmiş olup “gri kutu” (grey box) olarak nitelendirilmektedir. Bu sebeple test sonucunda mantıksal güvenlik açıklıkları, olası güvenlik açıkları, yanlış yapılandırmalar, savunma önlemlerinin eksikliklerinin tespiti için kapsamlı bir çalışma ortamı olarak düşünülebilir.

Testler, ekmek Bilgi Teknolojileri sızma testi ekibi tarafından gerçekleştirilmiştir. Testler sırasında çeşitli ticari tarama ürünleri, herkes tarafından temin edilebilecek açık kaynak kodlu programlar ve ekip tarafından geliştirilmiş yardımcı program ve araçlar kullanılmıştır.

Bu raporda gerçekleştirilen sızma testleri, tanımlanan kullanıcı profilleri ile belirlenen erişim noktalarına yönelik gerçekleştirilmiştir. Testler, **sistem tespiti**, **servis tespiti** ve **açıklık taraması/araştırması** adımları ile başlamış, ardından her bir erişim noktası için uygun adımlar doğrultusunda devam etmiştir.

Testlerin yapılış şekli genel metodolojiye göre kurgulanmıştır. Buna göre;

Test, kurumun **iç ağında** bulunan belirli IP adreslerini hedef almıştır. Kullanıcı VLAN’ı üzerinden gerçekleştirilmiştir.

Web uygulama testi, OWASP Top 10 güvenlik açıkları (örneğin, SQL Injection, XSS, CSRF, kimlik doğrulama zafiyetleri vb.) temel alınarak detaylı testler gerçekleştirilmiştir. Test edilen uygulamalar, kurum tarafından sağlanan alan adları ve IP adresleri üzerinden, kurumun mobil uygulamaları (Android ve iOS platformlarında) test edilmiştir. Mobil uygulamaların API güvenliği, veri şifreleme, sertifika doğrulama ve istemci tarafı zafiyetleri analiz edilmiştir. Testler, uygulamanın iletişim kurduğu API'lerin güvenlik açıklarını ve uygulamanın genel güvenlik yapısını değerlendirmeyi kapsamıştır.

DDos testleri yaparken esas amaç, gerekli saldırı ve ölçüm mekanizmalarını oluşturup, ilgili sistemin ve sistemlere hizmet veren internet servis sağlayıcının (ISS), dağıtık hizmet dışı bırakma saldırıları karşısında göstereceği tepkiyi gözlemlemek, sistem yoğun atak aldığında çıkabilecek problemlerini öngörmek ve kurumun dağıtık hizmet dışı bırakma saldırılarına karşı kurduğu sistemi iyileştirmek için gereken bilgiyi sağlamaktır.

Tüm test sürecinde, saptanan açıklık ve bulgular detaylı bir şekilde incelenmiş ve raporlanmıştır. Bulgular, kapsam bölümünde belirtilen başlıklarla ilişkilendirilerek analiz edilmiştir. Her bir test başlığı kapsamında tespit edilen açıklıklar, bağımsız olarak değerlendirilmiş, ayrıca bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da analiz edilmiştir. Bu kapsamda, birleştirilmiş değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporun bulgular bölümüne eklenmiştir.

**Bulgu Değerlendirme Süreci**  
Bulgular, raporun **"Bulgu Önem Dereceleri"** kısmında açıklanan sınıflandırma ve değerlendirme kriterleri kullanılarak analiz edilmiştir. Bu değerlendirme sürecinde, bulgu önem dereceleri belirlenirken varlığın değeri göz önünde bulundurulmamıştır. Varlıkların önceliklendirilmesi ve önem derecelerine göre aksiyon alınması, **Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır.**

**Koordinasyon ve Hizmet Kesintisinin Önlenmesi**  
Sızma testleri planlanırken ve uygulanırken, kurum ve kuruluşların iş sürekliliği dikkate alınmış, faaliyetlerin kesintiye uğramaması için gerekli önlemler alınmıştır. Hizmet kesintisine neden olabilecek test adımları, kurum ile koordinasyon sağlanarak dikkatle planlanmıştır. Böylece kritik işlemler ve sistemlerin aksamaması hedeflenmiştir.

Bu metodoloji, sızma testlerinin etkin bir şekilde gerçekleştirilmesini ve güvenlik açıklarının kapsamlı bir şekilde değerlendirilmesini sağlamıştır.

#### Testlerin Gerçekleştirildiği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği erişim noktaları, aşağıda tanımlanan alanlar çerçevesinde ele alınmıştır. Bu noktalara erişim sağlandıktan sonra belirlenen adımlarla sızma testleri gerçekleştirilmiştir.

1. **İnternet Üzerinden Erişim**Kurum, Kuruluş ve Ortaklıkların internet üzerinden erişilebilir durumda olan ve sadece kapsamda belirtilmiş olan sunucu ve servislerine erişim sağlanmıştır. İnternet tabanlı bu sistemlere yönelik sızma testleri gerçekleştirilmiş ve sistemlerin güvenlik durumu detaylı olarak incelenmiştir.
2. **Kurum,** **Kuruluş ve Ortaklıklar İç Ağı**  
   Kurum, Kuruluş ve Ortaklıkların iç ağında yer alan ve test kapsamına dahil edilen sistemler üzerinde çalışmalar gerçekleştirilmiştir. Bu İç ağda yapılan bu testler sırasında ağ trafiği üzerinde gerçekleştirilmesi planlanan testler için, kurumun genel çalışan bilgisayar profillerini yansıtan cihazlar kullanılmıştır.

#### Testlerin Gerçekleştiği Kullanıcı Profilleri:

1. Anonim kullanıcı profili,
2. Kurum, kuruluş ve ortaklıkları ve müşterisi profili,
3. Kurum, kuruluş ve ortaklıklar çalışanı profilleri üzerinden gerçekleşmiştir.

|  |
| --- |
| **Kurum, Kuruluş Ortakları Çalışan Profili:**   * Test Kullanıcısı:Estt\a\*\*\*\*.\*\*\*\*\*\*\*\* * Parola:U\*\*\*\*\*\*\*\*\*   **Kurum, Kuruluş Ortakları Müşterisi Profili:**   * Hesap numarası: 8\*\*\* * Parola: 1\*\*\*\*\* * SMS Kodu: 1\*\*\*\*\* |

#### Sistem Tespiti, Servis Tespiti Ve Açıklık Taraması

Gerçekleştirilen sızma testleri sırasında, metodoloji kapsamında sistem tespiti, servis tespiti ve açıklık taraması adımları uygulanmıştır. Bu adımlar aşağıdaki şekilde gerçekleştirilmiştir:

#### Sistem Tespiti

Sunucu veya aktif/pasif ağ cihazlarının sistem/yapılandırma bilgileri tespit edilerek çalışılmıştır.

#### Servis Tespiti

Kurum, kuruluş ve ortaklıklar bünyesindeki bilgi sistemlerinde yer alan varlıkların port taramaları yapılmış; internet/dünya genelinde erişime açık portlar ve sundukları servisler tespit edilmeye çalışılmıştır.

#### Açıklık Taraması/Araştırması

Kurum, kuruluş ve ortaklıkların bileşenleri ile bu bileşenlerin sunduğu servisler, güncel açıklıklara karşı taranmış ve muhtemel güvenlik açıkları belirlenmeye çalışılmıştır. Ayrıca tespit edilen açıklıklar, açıklık veritabanları gibi kaynaklar kullanılarak detaylı bir şekilde analiz edilmiştir. Açıklıkların ileşenler ve bileşenlerin etkileşimde olduğu sistemler üzerindeki güvenlik etkileri araştırılmıştır.

#### Sızma Testleri

Sızma testleri, Kurum, Kuruluş ve Ortaklıkların internet üzerindeki varlıklarına ve iç ağlarına yönelik olarak gerçekleştirilmiştir. Testlerin kapsamı ve detayları aşağıda açıklanmıştır:

#### İnternet Üzerinden Gerçekleştirilen Temel Sızma Testleri

Kurum, Kuruluş ve Ortaklıklar ağı dışından, bağımsız bir lokasyondan internet üzerindeki IP adresleri ve sunucular taranmıştır. Buna göre:

* Sistem Tespiti: İnternet üzerindeki varlıkların genel durumu analiz edilmiştir.
* Servis Tespiti: Çalışmakta olan servisler ve sürümleri belirlenmiştir.
* Açıklık Taraması: Belirlenen varlıklar üzerinde bilinen güvenlik açıkları taranmış ve detaylı analizler gerçekleştirilmiştir.

#### Kurum, Kuruluş ve Ortaklıkların İç Ağından Gerçekleştirilen Sızma Testleri

Kurum, Kuruluş ve Ortaklıkların iç ağına yönelik olarak gerçekleştirilen testler sırasında, sistem tespiti, servis tespiti ve açıklık taramasının yanı sıra aşağıdaki adımlar uygulanmıştır:

* Kurum Yerel Ağ Haritası Tespiti: İç ağdaki cihazların ve altyapının aktif portları çıkarılmıştır.
* Açık Portlar Üzerinden Testler: Belirlenen açık portlar üzerinde içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma (data exfiltration) gibi testler gerçekleştirilmiştir.
* Yerel Alan Ağı Zafiyet Taraması: İç ağda mevcut güvenlik açıkları belirlenmiş ve analiz edilmiştir.
* Araya Girme Teknikleri: Hassasiyet derecesi yüksek bilgiler elde edilmek üzere araya girme (Man-in-the-Middle) teknikleri denenmiştir.
* Bilgi Tabanlı Saldırılar: Elde edilen bilgiler ışığında kapsama dahil olan sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırıları yapılmıştır.

### Öneriler

#### Güvenlik İyileştirmeleri

* LDAP üzerinden gerçekleştirilen sorguların şifrelenmesi için LDAPS kullanılmalı.
* SIEM, EDR ve DLP gibi araçlardan gelen verileri kullanarak proaktif tehdit avlama süreçleri başlatılabilir.
* Dynamic Access Control (DAC) uygulayarak dosya ve klasör erişimleri sürekli olarak yeniden doğrulama ile kontrol edilmelidir.
* Kurum içerisinde ağ ve kullanıcı davranışlarını analiz etmek için makine öğrenimi algoritmaları kullanılabilir.
* Hassas verilerin tamamen izole edilmiş bir ortamda tutulması sağlanmalıdır.
* File Integrity Monitoring gibi yazılımlarla çalışan uygulamalar ve dosya sistemleri üzerinde gerçek zamanlı davranış analizleri izlenebilir.
* Tedarik zincirinden kaynaklanabilecek risklere karşı denetimler yapılarak tedarikçi güvenlik politikalarının kurum politikalarıyla uyumlu olması sağlanmalıdır.
* Sistemler kullanıcı bloğundan durdurulamayacak kadar sıkılaştırılmış olsada, olağanüstü durumlar için hızlı kurtarma planları geliştirilmelidir.
* Düzenli segmentasyon testleri ve ağ izleme yapılmalıdır.
* Tüm erişim kurallarının periyodik olarak gözden geçirilmesi ve güncellenmesi işlemleri rutin olarak yapılmalıdır.

### Sonuç

#### Test Sonuçları ve Genel Değerlendirme Kurum içindeki sistemlerin sıkı bir güvenlik politikasıyla yönetildiği gözlemlenmiştir. Testler sırasında ve ağ üzerinde herhangi bir yetkisiz erişim sağlanamadığı tespit edilmiştir.

Bu durum, kurumun aşağıdaki güvenlik hedeflerini başarıyla karşıladığını göstermektedir:

Kullanıcıların ağda potansiyel saldırı veya bilgi toplama amacıyla kullanılan araçları çalıştıramadığı doğrulanmıştır. Bu, zararlı aktivitelerin minimize edildiğine işaret eder.

Kullanıcı bloğunda, yalnızca belirlenen izinlere sahip işlemlerin gerçekleştirilebildiği gözlemlenmiştir. Bu, sistemlerin yalnızca iş amaçlı kullanılmasına yönelik sıkı politikaların uygulandığını göstermektedir.

Yetkisiz komutların veya araçların engellenmesi, etkin bir güvenlik izleme ve kontrol mekanizmasının mevcut olduğunu işaret etmektedir. Bu, kurumun genel güvenlik duruşunu güçlendiren önemli bir faktördür.

Özetle, kurum içindeki sıkılaştırma politikası hem kullanıcı hem de sistem düzeyinde proaktif bir şekilde uygulanmaktadır. Bu durum, yetkisiz erişimlerin ve araç kullanımının önlenmesi açısından etkili bir koruma sağlamaktadır. Mevcut politikaların bu şekilde devam ettirilmesi önerilmektedir.

### Bulgu Önem Dereceleri

Bulunan her güvenlik açığı veya sistemler hakkında bilgi toplamaya yarayan her türlü bilgi sızıntısı, kurumun bilgi sistemlerinin güvenliği için oluşturduğu tehdit açısından önem sırasına göre değerlendirilmelidir. Her kurumun kaynakları sınırlı olduğuna göre, bulunan güvenlik kapatmak için harcanacak olan kaynakların bu önem sırasına göre ayrılması gerekir. Yapılan çalışma sonucunda ortaya çıkarılan güvenlik açıkları, aşağıda anlatılan yöntem ve kıstaslarına göre sınıflandırılmıştır.

Bulunan güvenlik açıkları, önem seviyesi Acil, Kritik, Yüksek, Orta, Düşük olmak üzere belirlenmiştir. Acil ya da Kritik öneme sahip açıklıklar sonuç raporu beklenmeden hemen standart bir form aracılığıyla sorumlular ile paylaşılır.

Raporda yer alan her bir güvenlik açığına, yukarıda anlatılan önem derecelerinden biri atanır. Önem derecelerinin açıklamaları aşağıdaki tablolardan incelenebilir.

|  |  |
| --- | --- |
| **Önem Derecesi** | **Açıklama** |
| **ACİL** | Niteliksiz saldırgan tarafından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklardır. |
| **KRİTİK** | Nitelikli saldırgan tarafından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklardır. |
| **YÜKSEK** | Kuruluş dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklardır. |
| **ORTA** | Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklardır. |
| **DÜŞÜK** | Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir. |

# İletişim Altyapısı ve Aktif Cihazlar

İletişim Altyapısı ve Aktif Cihazlara yönelik güvenlik denetim adımları genel olarak aşağıdaki başlıklar altında gerçekleştirilmiştir:

* Yönlendiricinin işletim sisteminin barındırdığı bulguların araştırılması.
* Tespit edilen açıkların uygulanabilirliklerinin sınanması
* Anahtar üzerindeki VLAN ve trunk yapısının denetlenmesi
* Arp,dns zehirlenmesive spofing testlerin denetlenmesi
* Anahtar üzerindeki port güvenliğinin denetlenmesi
* Tüm ağ cihazlarıbulgubulma araçları ile taranmıştır. Tespit edilen açıkların uygulanabilirlikleri sınanmıştır.
* Cihazlar üzerinde açık olan servislerine kaba güç kullanılarak erişim sağlanmaya çalışılmıştır.
* Kaba kuvvet testleri ve zafiyetlerin denetlenmesi
* Yönlendirici uzaktan yönetim mekanizmasının denetlenmesi
* Yönlendirici ve Anahtar kayıt mekanizmasının incelenmesi
* Yönlendirici ve Anahtar Bulgubulma araçları ile taranması
* Vlan Segmentasyon Testleri gerçekleştirilmiştir.
* Yönlendirici ve Anahtar kimlik doğrulama mekanizmalarının denetlenmesi
* Anahtara uzaktan ve lokalden erişim kontrol mekanizmalarının denetlenmesi
* Yönlendirici ve Anahtar üzerinde çalışan servislerin denetlenmesi
* Yönlendirici üzerindeki parola saklama mekanizmalarının denetlenmesi
* Yönlendirici erişim kontrol listelerinin denetlenmesi

|  |  |
| --- | --- |
| **Bulgu Referans No:** | **IA001** |
| Bulgu Adı: | SNMP Ajanında Varsayılan Olarak “Public” Kullanılması |
| Önem Derecesi : | Orta |
| Etkisi: | Yetkisiz Erişim, Bilgi İfşası |
| Erişim Noktası: | Kurum, Kuruluş ve Ortaklıklar İç Ağı |
| Kullanıcı Profili: | Kurum, Kuruluş ve Ortaklıklar Çalışanı Profili |
| Bulgunun Tespit Edildiği Bilgi Sistemi Bileşen/Bileşenleri: | **161 / udp / snmp**  172.16.0.117 172.16.0.118 |
| Bulgu Açıklaması: | Hedef sistemde veya ağ cihazında çalışan SNMP (Simple Network Management Protocol) hizmetinin public adlı varsayılan topluluk adı (community string) ile yapılandırıldığı tespit edilmiştir. Bu durum, saldırganların yetkisiz erişimle sistem bilgilerini sorgulamalarına olanak tanır.   * Okuma izni verilen varsayılan topluluk adıdır ve birçok cihazda ilk yapılandırmada kullanılmaktadır. Bu, kolayca tahmin edilebilir ve potansiyel bir güvenlik açığı oluşturur. * Ağ cihazlarının yapılandırma bilgileri (ör. IP adresleri, cihaz türleri, çalışma durumu) saldırganlar tarafından sorgulanabilir. * Hassas bilgiler ele geçirilebilir veya cihazlar kötüye kullanılabilir.   Bulgu.image |
| Çözüm Önerisi: | * Public topluluk adını karmaşık bir topluluk adı ile değiştirin * SNMPv1 veya SNMPv2 yerine, şifreleme ve kimlik doğrulama sağlayan **SNMPv3**'e geçiş yapın. * SNMP erişimini yalnızca yetkili IP adresleriyle sınırlandırın. |

# DNS Servisleri

• DNS sunuculara aşağıdaki güvenlik denetim adımları gerçekleştirilmiştir:

• DNS sunucuların topolojik konumunun incelenmesi

• DNS Sunucusunun alan yapılandırmasında yer alan kayıtların ortaya çıkarılmaya çalışılması

• DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılması

• DNS sunucular üzerindeki kaynak kayıt girdilerinin incelenmesi

• DNS sunucuların sürüm bilgisinin elde edilmeye çalışılması

• Müşteri Kurum dışı alan isimlerinin sorgulanmaya çalışılması

• Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığının incelenmesi Güvenlik Duvarında DNS sunucular için izin verilen portların incelenmesi

• DNS sunucuların güvenlik taramasına tabi tutulması

• Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılması

• NXT ve NSEC kaynak kayıtları üzerinden bilgiler elde edilmeye çalışılması

• Netcraft, Google, Whois sorguları yapılarak Müşteri Kurum alanında yer alan sunucuların tespit edilmeye çalışılması

• DNS servisini veren yazılımın açıklıklarının araştırılması

**\* Bulgu tespit edilememiştir.\***

# Etki Alanı ve Kullanıcı Bilgisayarları

Etki alanı sunucularında ve son kullanıcı bilgisayarlarında aşağıdaki güvenlik denetim adımları gerçekleştirilmiştir

* Etki alanı sunucularında ve son kullanıcı bilgisayarlarında aşağıdaki güvenlik denetim adımları gerçekleştirilmiştir.
* Sunucu ve kullanıcı bilgisayarlarında hassas bilgi içeren ve yetkisiz erişime olanak sağlayan paylaşımlar kontrol edilmiştir.
* Sunucu ve kullanıcı bilgisayarlarında taşınabilir aygıtların kullanımı ile ilgili güvenlik ayarları kontrol edilmiştir.
* Etki alanında uygulanan şifre, hesap kilitleme politikaları kontrol edilmiştir.
* Etki alanındaki yetkili kullanıcıların ayrıcalıkları ve kullanım şekilleri kontrol edilmiştir.
* Sunucu ve kullanıcı bilgisayarlarında uygulanan yama yönetimi politikaları kontrol edilmiştir.
* Sunucu ve kullanıcı bilgisayarlarında uygulanan virüs koruma politikaları kontrol edilmiştir.
* Sunucu ve kullanıcı bilgisayarlarındaki yerel kullanıcı hesabı ve kullanıcı grupları kontrol edilmiştir.
* Kullanıcı bilgisayarların fiziksel saldırılara karşı güvenilirliği kontrol edilmiştir.

|  |  |
| --- | --- |
| **Bulgu Referans No:** | **EA001** |
| Bulgu Adı: | Desteklenmeyen Yazılım/Servislerin Kullanımı |
| Önem Derecesi : | Yüksek |
| Etkisi: | Bilgi sızıntısı, yetkisiz erişim ve hizmet kesintisi |
| Erişim Noktası: | Kurum, Kuruluş ve Ortaklıklar İç Ağı |
| Kullanıcı Profili: | Kurum, Kuruluş ve Ortaklıklar Çalışanı Profili |
| Bulgunun Tespit Edildiği Bilgi Sistemi Bileşen/Bileşenleri: | **Python**  **4000-40001-40002-40003/5000/7000 / tcp / www**  172.16.0.91 172.16.0.95  **1717 / tcp / www**  172.16.0.75  **vCenter**  **443 / tcp / www**  172.16.0.10 |
| Bulgu Açıklaması: | **Python 3.6.9**:   * Python 3.6 serisinin desteği **31 Aralık 2021** tarihinde sona ermiştir. * Python 3.6.9 üzerinde bilinen güvenlik açıkları (ör. kütüphane zafiyetleri, güvenlik güncellemelerinin eksikliği) sömürülebilir. Ayrıca kütüphanelerle uyum sorunları yaşanabilir.   **vCenter 7.0.3**:   * Bu sürümde bilinen güvenlik açıkları (ör. CVE-2021-21985, CVE-2021-22005) sistemin yetkisiz erişimlere ve bilgi sızıntısına açık hale gelmesine neden olabilir.   172.16.0.75 |
| Çözüm Önerisi: | **Python 3.6.9 Güncellemesi**:   * Python'u **3.9** veya daha yeni bir LTS sürümüne yükseltin.   **vCenter 7.0.3 Güncellemesi**:   * VMware tarafından sağlanan en son **vCenter Server** sürümüne yükseltin. * Güncelleme işlemi öncesinde tüm veritabanı ve ayarların yedeklerini alın. * Kritik zafiyetleri gidermek için güvenlik yamalarını uygulayın. |

# E-posta Servisleri

• E-posta sunuculara yapılan testler aşağıda listelenmiştir.

• E-posta sunucularının topolojik konumu incelenmiştir.

• E-posta sunucular açıklık taramasına tabi tutulmuştur.

• Sistemlerde kullanılan e-posta içerik kontrolcüleri, anti-virüs ağ geçitleri, spam filtrelerinin kullandığı kütüphanelerde var olabilecek muhtemel açıklıklar incelenmiştir. E-posta servisini veren yazılımların bilinen diğer açıklıkları araştırılmıştır.

• E-posta servislerinin gönderilen e-postaların boyutlarını sınırlayıp sınırlamadığını kontrol etmek amacı ile boyutu büyük e-postalar gönderilmiştir.

• Muhtemel olarak kullanılan e-posta listesi yazılımlarının açıklıkları tespit edilmeye çalışılmıştır.

• Virüs tarayıcı ağ geçitlerinin sürüm bilgisi elde edilmeye çalışılacak bu sürümlerin bilinen açıklıkları araştırılmıştır.

• Sunucular üzerindeki yönlendirme (relaying) zafiyetlerini incelemek için bir dizi e- posta gönderilmiştir.

• E-posta servislerinin gönderilen e-postaların boyutlarını sınırlayıp sınırlamadığını kontrol etmek amacı ile boyutu büyük e-postalar gönderilmiştir.

• Muhtemel olarak kullanılan e-posta listesi yazılımlarının açıklıkları tespit edilmeye çalışılmıştır.

• Sunucular üzerinde e-posta dışında bir servisin çalışıp çalışmadığı incelenmiştir.

• E-posta sunucu üzerinde kimlik doğrulamanın aktif olup olmadığı incelenmiştir. E-posta sunucu üzerinde POP3, IMAP gibi istemci servislerinin erişime açık olup olmadığı kontrol edilmiştir.

**\* Bulgu tespit edilememiştir.\***

# Veri Tabanı Servisleri

Veri tabanı yönetim sistemleri üzerinde aşağıdaki güvenlik denetim adımları gerçekleştirilmiştir.

* Veri tabanı yönetim sistemleri üzerinde yapılan güvenlik denetimleri aşağıdaki genel başlıklarda incelenmiştir.
* Veri tabanı sunucusunun fiziksel konumu ve güvenlik açısından etkilenebileceği çevresel faktörler incelenmiştir.
* Sistemde fonksiyonelliği bozmayacak olan güncel sistem ve güvenlik yamalarının uygulanıp uygulanmadığı kontrol edilmiştir.
* Veri tabanı sunucusunda, denetleme mekanizmasının aktif olup olmadığı incelenmiştir.
* Veri tabanı sunucusunun yedekleme ve kurtarma mekanizması incelenmiştir.
* Veri tabanının kurulumu ile birlikte gelen ve kullanıcılar için atanan varsayılan değerler kontrol edilmiştir.
* Veri tabanı sunucularına uzaktan erişimin güvenli olup olmadığı kontrol edilmiştir
* Veri tabanı için önemli olan işletim sistemi dosyalarının erişim izinleri kontrol edilmiştir.

**\* Bulgu tespit edilememiştir.\***

# Web Uygulama Testleri

Web ve Mobil uygulamalara yönelik aşağıdaki güvenlik denetim adımları gerçekleştirilmiştir:

* SSL/TLS protokolü yapılandırmasının güvenli algoritmalar kullanıp kullanmadığının incelenmesi.
* Eksik veya yanlış yapılandırılmış HTTP güvenlik başlıklarının tespit edilmesi.
* Uygulama ile sunucu arasındaki trafiğin güvenliğini sağlayan pinning koruma mekanizmalarının test edilmesi.
* İki faktörlü kimlik doğrulama (2FA) önlemlerinin kaba kuvvet saldırılarına karşı dayanıklılığının değerlendirilmesi.
* Sunucu taraflı kontrol eksikliklerinin kullanıcı yetkilendirmesi üzerindeki etkilerinin incelenmesi.
* Uygulama üzerinde depolanan hassas bilgilerin açık metin olarak saklanıp saklanmadığının kontrol edilmesi.
* Maskelenmesi gereken hassas bilgilerin (parola, kredi kartı bilgileri vb.) doğru bir şekilde gizlenip gizlenmediğinin incelenmesi.
* Veri sızıntısı tespiti için uygulama ve API kaynaklarının analiz edilmesi.
* Uygulama üzerinde sınırsız form ve e-posta gönderimi gibi işlem sınırlandırmalarının test edilmesi.
* Bağımlılık ve sürüm bilgilerinin açıkça erişilebilir olup olmadığının kontrol edilmesi.
* Kullanıcı girdilerinin sunucu tarafında doğru bir şekilde kontrol edilip edilmediğinin analiz edilmesi.
* Güvensiz veri depolama yöntemlerinin tespit edilmesi ve bu durumun uygulama işleyişine etkilerinin değerlendirilmesi.
* Eksik veya güvenli olmayan uygulama protokollerinin incelenmesi.

|  |  |
| --- | --- |
| **Referans No:** | **WE001** |
| Bulgu Adı: | SSL Şifreleme Algoritmasında Güvenli Sayılmayan Algoritma Kullanılması |
| Önem Derecesi: | Düşük |
| Etkisi: | Bilgi ifşası |
| Erişim Noktası: | İnternet |
| Kullanıcı Profili: | Anonim |
| Bulgunun Tespit Edildiği Bilgi Sistemi Bileşen/Bileşenleri: | Esttaz.com.tr:443/tcp  esube.esttatz.com.tr:443/tcp  mail.Esttaz.com.tr:443/tcp  onlinehesapac.Esttaz.com.tr:443/tcp |
| Bulgu Açıklaması: | Zayıf anahtar (weak cipher) kullanımı, Ortadaki Adam (man in the middle) olarak adlandırdığımız saldırı çeşidine; iletişim sırasında gönderilen ve alınan bütün verilerin okunmasına, kaydedilmesine ve/veya değiştirilmesine sebebiyet verebilir. İnternet’e açık veritabanlarında daha önceden çözümlenmiş ve çakışma içeren anahtarların kullanılması şifreli trafiği çözmeye ve tüm verilerin üçüncü taraflarca görünür olmasına olanak tanır.  Saldırgan şifreli trafiği ele geçirip şifreleme algoritmasındaki zayıf anahtarları çözümleyerek trafiği düz metin hale getirebilmektedir.  Yapılan incelemelerde artık geçerliliğini yitirmiş şifreleme algoritmalarının kullanıldığı tespit edilmiştir |
| Çözüm Önerisi: | 30 Haziran 2018’den sonra TLS v1.0 ve SSL v3.0 protokollerinin kullanılmaması gerekmektedir. TLS v1.0 ve SSL v3 gibi çakışma içeren ve güvenilirliği şüpheli olan protokollerinin sunucu tarafta kabul edilmemesi önerilir.  https://www.owasp.org/index.php/Testing\_for\_Weak\_SSL/TLS\_Ciphers,\_Insufficient\_Transport\_Layer\_Protection\_(OTG-CRYPST-001)  https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/ |

# Mobil Uygulama Testleri

* Websocket parolalarının açık metin olarak saklanıp saklanmadığının kontrol edilmesi.
* Kaynak tüketen HTTP isteklerinin sınırsız şekilde yapılabilip yapılamadığının test edilmesi.
* Uygulama üzerindeki ROOT kontrolünün atlatılıp atlatılamadığının kontrol edilmesi.
* Pinning mekanizmalarının atlatılabilir olup olmadığının test edilmesi.
* Mobil uygulamanın cihaz üzerinde açık metin veri depolayıp depolamadığının incelenmesi.
* Mobil uygulama ile sunucu arasındaki iletişimde şifreleme mekanizmalarının etkinliği ve güvenilirliği test edilmiştir.

|  |  |
| --- | --- |
| **Bulgu Referans No:** | **MB001** |
| Buldu Adı: | Websocket Parolasının Açık Metin Olarak Saklanması |
| Önem Derecesi: | Kritik |
| Etkisi: | Bilgi İfşası ve Yetkisiz Erişim |
| Erişim Noktası: | İnternet |
| Kullanıcı Profili: | Kurum, kuruluş ve ortaklıkları ve müşterisi profili |
| Bulgunun Etki Ettiği/Edebileceği Bileşen/Bileşenler: | com.Esttaz.mobil - EsttAZ Borsa [Android] |
| Bulgu Açıklaması: | Mobil uygulama üzerinde yapılan güvenlik testlerinde, bir *memory dump* (bellek dökümü) alındığında, uygulamanın WebSocket bağlantısı için kullanılan parolanın açık metin (plain text) olarak bellek içinde tutulduğu gözlemlenmiştir. Bu durum, parolanın güvenliği açısından ciddi bir risk oluşturur, çünkü bir saldırgan bu tür bir bellek dökümünü ele geçirirse, parolayı doğrudan erişebilir ve bu sayede yetkisiz WebSocket bağlantıları kurarak uygulamanın veri akışına müdahale edebilir. Ayrıca, uygulama veritabanı veya sunucu üzerindeki kaynaklara da yetkisiz erişim sağlanabilir.  Aşağıdaki görselde SOCKET\_PASSWORD bölümünde parola görüntülenmektedir.  wss://ws-test-mbl.foreks.com/websocket |
| Çözüm Önerisi: | WebSocket parolasının açık metin olarak bellekte tutulmasının önlenmesi için uygulamanın parolayı şifreli bir şekilde saklaması gerekmektedir. Bu amaçla, parola hiçbir zaman doğrudan bellek içinde tutulmamalıdır. Parola, güçlü bir şifreleme algoritması kullanılarak (örneğin AES) şifrelenmeli ve şifreli haliyle güvenli bir alanda saklanmalıdır. Uygulama, şifreli parolayı geçici olarak güvenli bir depolama alanında tutarak (Android için Keystore, iOS için Keychain gibi) bellekte açık metin halinde bulunmasını engellemelidir. Ayrıca, WebSocket oturumları için şifre yerine daha güvenli kimlik doğrulama yöntemleri tercih edilebilir. Örneğin, JWT (JSON Web Tokens) gibi token tabanlı doğrulama mekanizmaları kullanılabilir. Son olarak, parola ile işlem yapıldıktan sonra, bellekten tamamen temizlenmesi için güvenli bellek yönetimi teknikleri uygulanmalıdır.  Dumping Applications Memory  https://redfoxsec.com/blog/dumping-android-application-memory/ |

|  |  |  |
| --- | --- | --- |
|  |  |  |

# Kablosuz Ağ Sızma Testi

* Kurumda kullanılan kablosuz ağ cihazlarının genel mimari içindeki yerinin incelenmesi İstemcilerin kablosuz ağ yapılandırmalarının incelenmesi
* Kurumda bulunan kablosuz ağlar taranarak özelliklerinin keşfedilmeye çalışılması
* Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığının incelenmesi
* Kablosuz ağlarda kullanılan şifreleme ayarlarının incelenmesi
* WEP ve WPA/WPA2 şifreleme kullanılan ağlarda kablosuz ağ şifresinin ele geçirilmeye çalışılması
* Sahte kablosuz ağ erişim noktaları oluşturularak kurumda bulunan istemcilerin ele geçirilmeye çalışılması
* İstemciler üzerinden kablosuz ağ taraması yapılarak, kurum etrafında bulunan diğer kablosuz ağların keşfedilmeye çalışılması
* SSID olarak ESTTAZ, ESTTAZ\_WIFI, ESTTAZ\_MISAFIR keşfedilmiştir.
* DeAuth Saldırısı yapılmıştır. İlgili SSID’ler üzerinden yayın yapan AP düşürülememiştir.

\* Bulgu tespit edilememiştir.

# Dağıtık Servis Dışı Bırakma Testleri

* DDoS (Distributed Denialof Service) saldırılarının çeşitli teknik yöntemleri vardır ve bu yöntemler, siber saldırganların hedef sistemleri aşırı yüklemek veya erişilemez hale getirmek için kullandığı tekniklerin bir parçasını oluşturur. İşte bu tür saldırılarda kullanılan bazı teknikler:
* **Aşırı Paket Gönderimi (Traffic Flooding):**Saldırganlar, hedeflenen web sunucusuna veya ağ kaynaklarına aşırı miktarda ağ trafiği veya paket gönderirler. Bu, kaynakların bant genişliğini tüketerek hizmetlerin erişilemez hale gelmesine neden olur.
* **SYN Flood:**Bu, TCP/IP protokolünü hedef alan bir DDoS yöntemidir. Saldırganlar, hedef sunucuya çok sayıda TCP bağlantı isteği (SYN) gönderirler, ancak bu istekleri tamamlamazlar. Bu, sunucunun bağlantıları açık bırakmasına ve kaynakları tükenmesine neden olur.
* **Mail Sunucusu Saldırıları:**Herkese hizmet veren e-posta sunucuları, aşırı miktarda e-posta trafiği nedeniyle DoS ve DDoS saldırılarına karşı savunmasız olabilirler. Saldırganlar, hedef e-posta adreslerine aşırı miktarda e-posta göndererek bu saldırıları gerçekleştirirler.
* Uygulama Katmanı Saldırıları: Bu tür saldırılar, hedef uygulama sunucularını hedefler ve uygulamanın işleyişini bozar. Örnekler şunları içerir:
* **SLOW READ:**Saldırganlar, web sunucularına yavaş bir şekilde veri okuma isteği göndererek sunucunun kaynaklarını tüketirler.
* **SLOW BODY:**Saldırganlar, HTTP isteği gönderdikten sonra çok yavaş bir şekilde veri göndererek sunucunun kaynaklarını tüketirler.
* **RANGE:**Saldırganlar, web sunucularına çok sayıda istek göndererek belirli bir dosyanın farklı parçalarını isteyebilirler.
* **SLOW HEADERS:**Saldırganlar, HTTP başlıklarını çok yavaş bir şekilde göndererek sunucunun işlem hızını düşürebilirler.

Yapılan dağıtık hizmet dışı bırakma testlerinde Amerika, Avrupa ve Türkiye lokasyonlu IP adresleri kullanılarak HTTP(S) GET Flood, ICMP Flood ve DNS Query metotları kullanılmıştır. Gerçekleştirilen dağıtık hizmet dışı bırakma saldırısı senaryolarıyla sistemlerin ve DDOS korumasının saldırılar karşısında verdiği tepkileri ve alınan önlemler tespit edilmektedir.

Testler maksimum 200Mbps, 500 Mbps ve 900 Mbps bant genişliği kullanılarak gerçekleştirilmiştir. Toplam 12 test yapılmış, bu testlerin değerlendirilmesi ile elde edilen sonuçlar bir sonraki bölümde sunulmuştur.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Saldırı** | **Tarihi** | **Başlama Saati** | **Süre** | **Hedef** | **Bant Genişliği** | **Test Sonucu** |
| **1** | HTTPS(S) GET Flood | 07.12.2024 | 01:22 | 310sn | www.Esttaz.com.tr | 200Mbps | **KORUMA BAŞARILI**  (30 saniyelik gecikme gözlemlendi) |
| **2** | ICMP Flood | 07.12.2024 | 01:34 | 390sn | www.Esttaz.com.tr | 500Mbps | **KORUMA BAŞARILI** |
| **3** | DNS Query Flood | 07.12.2024 | 01:46 | 390sn | www.Esttaz.com.tr | 900Mbps | **KORUMA BAŞARILI** |
| **4** | HTTPS(S) GET Flood | 07.12.2024 | 01:59 | 330sn | esube.Esttaz.com.tr | 200Mbps | **KORUMA BAŞARILI** |
| **5** | ICMP Flood | 07.12.2024 | 02:07 | 390sn | esube.Esttaz.com.tr | 500Mbps | **KORUMA BAŞARILI** |
| **6** | DNS Query Flood | 07.12.2024 | 02:18 | 380sn | esube.Esttaz.com.tr | 900Mbps | **KORUMA BAŞARILI** |
| **7** | HTTPS(S) GET Flood | 07.12.2024 | 02.25 | 310sn | onlinehesapac.Esttaz.com.tr | 200Mbps | **KORUMA BAŞARILI** |
| **8** | ICMP Flood | 07.12.2024 | 02:33 | 390sn | onlinehesapac.Esttaz.com.tr | 500Mbps | **KORUMA BAŞARILI** |
| **9** | DNS Query Flood | 07.12.2024 | 02:40 | 390sn | onlinehesapac.Esttaz.com.tr | 900Mbps | **KORUMA BAŞARILI** |
| **10** | HTTPS(S) GET Flood | 07.12.2024 | 02:48 | 310sn | mail.Esttaz.com.tr | 200Mbps | **KORUMA BAŞARILI** |
| **11** | ICMP Flood | 07.12.2024 | 02:56 | 390sn | mail.Esttaz.com.tr | 500Mbps | **KORUMA BAŞARILI** |
| **12** | DNS Query Flood | 07.12.2024 | 03:03 | 390sn | mail.Esttaz.com.tr | 900Mbps | **KORUMA BAŞARILI** |

# Sosyal Mühendislik Güvenlik Testi

* Sosyal ağlar, arama motorları, Müşteri Kurum web siteleri kullanılarak Müşteri Kurum ve çalışanları hakkında bilgi elde edilmeye çalışılması.
* Müşteri Kurum içinden veya dışından gönderilecek e-postalar ile kullanıcı bilgisayarlarına sızma denemesi gerçekleştirilmesi.
* Müşteri Kurum'a sızabilmek için hazırlanan özel materyallerin kullanıcılar tarafından çalıştırılması amacıyla ortamlar hazırlanması.

EsttAZ kurum çalışanlarına, “mail servislerine başka bir lokasyondan erişim sağlandığına” dair aşağıdaki oltalama şablonu kullanıldı. Sahte konum, Ip adresi ve program bilgileri ile kullanıcı yanıltılmaya çalışıldı. “Hesaba giriş parolasının ele geçirilmesi” lafzıylada kullanıcının panik yaparak ilgili linke tıklaması ve parolasını değiştirmesi için veri girişi yapması amaçlandı. Bu senaryo eşliğinde yapılan oltalama testi sonunda hiçbir kullanıcı zararlı linke tıklamadı.

|  |  |
| --- | --- |
| **Parametre** | **Sonuç** |
| Toplam Kullanıcı Sayısı | 104 |
| Zararlı Linke Tıklayan Kullanıcı Sayıs | 0 |
| Zararlı Linke Tıklama Oranı | %0 |
| Ransomware Zararı Görme İhtimali | %0 |

# Tüm Bulguların Birlikte Değerlendirilmesi

Gerçekleştirilen sızma testi kapsamında elde edilen tüm bulgular ayrı ayrı ve birlikte değerlendirilmiş olup birlikte değerlendirildiğinde herhangi bir güvenlik zafiyeti oluşturmadığı belirlenmiştir.

### 2023 Yılı Bulgu Özet Tablosu

|  |  |  |  |
| --- | --- | --- | --- |
| **Bulgu Referans No** | **Bulgu Adı** | **Bulgu Önem Derecesi** | **Doğrulama Denetim Sonucu** |
| IA-01 | Avaya Komut Enjeksiyonu | ACİL | **KAPATILMIŞTIR** |
| VT-01 | Microsoft SQL Sunucu Desteklenmeyen Sürüm | YÜKSEK | **KAPATILMIŞTIR** |
| EA-01 | Windows 7 MS17-010 Zafiyeti | ACİL | **KAPATILMIŞTIR** |
| EA-02 | VIVOTEK NETWORK CAMERA PRIOR XXXXXX-VVTK-0X09A  MOD\_INETD.CGI URL Erişim  Kontrolü | ACİL | **KAPATILMIŞTIR** |
| EA-03 | VATOS DLP Varsayılan Şifre | ACİL | **KAPATILMIŞTIR** |
| EA-04 | Microsoft Message Queuing RCE (MSMQ) | ACİL | **KAPATILMIŞTIR** |
| EA-05 | ESXi 6.5 / 6.7 / 7.0 | ACİL | **KAPATILMIŞTIR** |
| EA-06 | Ubuntu 16.04, 18.04, 20.04, 22.04 Sürümlerinde Çoklu Zafiyet | ACİL | **KAPATILMIŞTIR** |
| EA-07 | OpenSSL Güvenlik Açıkları | ACİL | **KAPATILMIŞTIR** |
| EA-08 | Apache ve PHP Zafiyetleri | ACİL | **KAPATILMIŞTIR** |
| EA-09 | Desteklenmeyen Windows İşletim  Sistemleri | ACİL | **KAPATILMIŞTIR** |
| EA-10 | NodeJS Sistem Komut Enjeksiyon | ACİL | **KAPATILMIŞTIR** |
| EA-11 | Redis Sunucusu Desteklenmeyen Parola Doğrulaması | KRİTİK | **KAPATILMIŞTIR** |
| EA-12 | Linux Sudo ile Yetki Yükseltme | KRİTİK | **KAPATILMIŞTIR** |
| EA-13 | SMB İmzalaması Olmadan Doğrulama Zafiyeti | YÜKSEK | **KAPATILMIŞTIR** |
| MOB-01 | Mobil Uygulamalarda SSL Sabitleme  Zafiyeti | KRİTİK | **KAPATILMIŞTIR** |
| MOB-02 | Hassas Bilgi İfşası | YÜKSEK | **KAPATILMIŞTIR** |
| MOB-03 | Base64 Kodlamasıyla Kimlik Doğrulama | ORTA | **KAPATILMIŞTIR** |

# Kullanılan Araçlar

Raporda detayları sunulan sunuculara doğru gerçekleştirilen testlerde aşağıdaki listelenen ticari ve açık kaynak kodlu araçların ilgili olanları kullanılmıştır.

**Ağ Tarayıcıları**

Nessus

OPENVAS

Metasploit Express / Rapid7

Nmap / Insecure.org

Netscan / Softperfect

**Diğer Araçlar**

Netsparker Mavituna / Security

Nikto2 / Cirt

Sqlmap / Sqlmap, sourceforge

OwaspZAP / Açık Kaynak Kodlu

Xenotix / Açık Kaynak Kodlu

Dirbuster / Açık Kaynak Kodlu

Wefuzz / Açık Kaynak Kodlu

WebCrusier / Açık Kaynak Kodlu

Telnet / UNIX Komutu

Traceroute / UNIX Komutu

Whois / UNIX Komutu

Dig UNIX / Komutu

Ripe.net / Kamuya Açık Web Sitesi

Dnsstuff.com / Kamuya Açık Web Sitesi

Exploit-db.com / Kamuya Açık Web Sitesi

Netcat / UNIX Komutu

Wireshark Açık Kaynak Kodlu

Kali Linux Araçları Açık Kaynak Kodlu