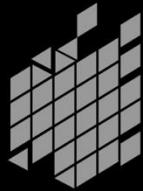


UITSEC BDDK Kapsamlı Penetrasyon Testi Örnek Raporu

Rapor No:

Rapor Sahibi:

Proje Yöneticisi:



UITSEC

More Secure Than Ever

13TH YEAR



BDDK UYUMLU PENETRASYON TESTİ RAPORU

Hakkımızda

2002 yılından bugüne, uygulama güvenliği, sistem – network güvenliği, kriptografi, adli bilişim ve kurumsal çözüm vizyonu ile hizmetine devam eden mühendislik ve danışmanlık firmamız, İstanbul Bebek'te bulunan genel merkezi ve Ankara'da bulunan teknik birim müdahale ofisi olmak üzere ülkemizde iki lokasyonda hizmet vermektedir. Bilgi ve bilişim güvenliği çerçevesinde 2002 yılından beri uluslararası anlamda çalışmaya devam eden firmamız, 3 ülkede ofisi bulunan bir marka haline gelmiştir.

BT yönetim hizmetlerinden, bilgi güvenliği iç denetimlerine, iş sürekliliği ve felaket kurtarma yönetiminden, bilişim hukuku danışmanlığına, penetrasyon testleri ve DOS/DDOS analizinden stres testlerine kadar bilgi-bilişim güvenliği, denetim ve yönetim alanında en iyi hizmeti kurumsal müşteri ve ortaklarına sunmaktadır.

Avrupa ve Amerika'da birçok firma ile çalışmış olan şirketimiz Türkiye ve Ortadoğu'nun en iyi holding ve firmalarına danışmanlık, denetmenlik, uzmanlık, güvenlik testi ve kurumsal farkındalık eğitimi hizmetini vermektedir. Ülkemizin, yurtdışında hizmet veren bilgi güvenliği ve siber güvenlik markası haline gelen firmamız, yurtdışındaki teknoloji enstitüleri ile beraber çalışmalar yapmakta, çalıştaylara katılmakta ve birçok uluslararası dernek ve oluşuma destek vermektedir. Sadece sunulan teknolojiyi kullanmanın dışında, yeni teknoloji üretmeyi ilke edinen UITSEC, danışmanlık ve mühendislik hizmeti sunduğu firmalara "Security Framework" vizyonunu kazandırmıştır.

Güvenilirlik ve Gizlilik politikası ile yoluna devam eden UITSEC (Universal IT Security Consulting), bilginin önemini farkında olan ve bu nedenle bilgi ve bilişim güvenliği hizmetlerini sizlere en iyi şekilde vermeye çalışan bir firmadır.

İÇİNDEKİLER TABLOSU

| | |
|--|----|
| HAKKIMIZDA | 3 |
| GİRİŞ..... | 5 |
| AMAÇ..... | 5 |
| KAPSAM..... | 5 |
| METODOLOJİ..... | 5 |
| Testlerin Gerçekleştirileceği Erişim Noktaları..... | 5 |
| Testlerin Gerçekleştirileceği Kullanıcı Profilleri..... | 6 |
| Sistem Tespiti, Servis Tespiti ve Açıklık Taraması | 6 |
| Temel Sızma Testleri..... | 6 |
| SIZMA TESTİ SONUÇLARININ TAKİBİ | 7 |
| GENEL DURUM VE GELİNEN SON DURUM | 7 |
| ZAFİYET TÜRLERİ | 7 |
| Bilgi İfşası..... | 7 |
| Yetki Yükseltme | 7 |
| Uzaktan Komut Çalıştırma | 8 |
| Servis Durdurma Zafiyetleri..... | 8 |
| ZAFİYET ETKİLERİ | 8 |
| TEHDİT SENARYOLARI | 8 |
| ZAFİYET DAĞILIMI | 9 |
| ZAFİYET SINIFLANDIRMA KRİTERLERİ | 10 |
| SIZMA TESTİ BULGULARI | 11 |
| Dış Test Bulguları | 11 |
| İç Test Bulguları..... | 19 |
| SIZMA KANITLARI | 25 |

GİRİŞ

Bu rapor [Firma İsmi] 'nin talebi üzerine [Tarih] tarihleri arasında verilen ve [bölüm sayısı] bölümünden oluşan Bilgi Sistemleri Penetrasyon Testi hizmetinin tamamlanması sonucu oluşturulmuş olup, raporlar müsterimiz olan [Firma İsmi]'ne "Yüksek Gizlilik" içeriği belirtilerek teslim edilmiştir.

Rapor kapsamında sunulmuş olan metod, bilgi ve açıklamalar UITSEC Firması'nın entelektüel varlığı olup hiçbir bölümü UITSEC Firması'nın yazılı izni olmadan değiştirilemez.

AMAÇ

Penetrasyon (Sızma) Testleri'nin amacı, kuruluşların bilgi sistemlerinde yetkisiz erişim kazanılmasına veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi ve sonrasında düzeltilmesidir.

KAPSAM

Sızma testleri; temel sızma testleri ve bu testlerin devamında uygulanacak olan detaylı sızma testlerinden oluşmaktadır. Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıklarını kapsamaktadır;

- a) İletişim Altyapısı ve Aktif Cihazlar
- b) DNS Servisleri
- c) Etki Alanı ve Kullanıcı Bilgisayarları
- d) E-posta Servisleri
- e) Veri Tabanı Sistemleri
- f) Web Uygulamaları
- g) Mobil Uygulamalar
- h) Kablosuz Ağ Sistemleri
- i) ATM Sistemleri
- j) Dağıtık Servis Dışı Bırakma Testleri
- k) Sosyal Mühendislik Testleri

METODOLOJİ

Sızma testleri, aşağıda detaylı bir şekilde anlatılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek temel sızma testleri ve detaylı sızma testlerinden oluşur. Temel sızma testleri sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar. Her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder.

Temel sızma testleri sonrası saptanan açıklık ve bulgular, kapsam bölümünde belirtilen ve ilişkili olduğu her bir başlık altında, detaylı sızma testlerinin gerçekleştirilmesi suretiyle ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular; ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir. Bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporlanır. Bu kapsamında bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak kurumun sorumluluğundadır.

Sızma testleri gerçekleştirilirken, kurumun faaliyetlerini aksatmayacak ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler kurum ile koordineli bir şekilde planlanarak gerçekleştirilir.

Testlerin Gerçekleştirileceği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği asgari erişim noktaları aşağıda tanımlanmaktadır. Bu noktalardan sisteme erişildikten sonra, temel sızma testleri gerçekleştirilmeli ve sonrasında detaylı sızma testleri uygulanmalıdır.

- i. **Internet:** Kurumun internet üzerinden erişilebilen tüm sunucu ve servislerine internet üzerinden erişilerek sızma testleri gerçekleştirilir.
- ii. **Kurum İç Ağı:** Kurumun iç ağında yer alan ve test kapsamında ele alınan sunuculara kurum iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağı trafiği üzerinde gerçekleştirilecek testler için de bu ağı kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarları profilinde bilgisayarlar sağlanır.

Testlerin Gerçekleştirilebileceği Kullanıcı Profilleri

Sızma testlerinin sağlıklı bir şekilde gerçekleştirilebilmesi ve testlerin gerçek hayatı uygun olması için, yukarıda tanımlanan erişim noktalarına bu ortamların doğasına uyacak şekilde aşağıdaki kullanıcı profilleri ile sızma testleri gerçekleştirilir.

- i. **Anonim Kullanıcı Profili:** Internet üzerinden, kurumun web servislerine erişilebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kuruma ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla profil kullanılmalıdır.
- ii. **Kurum Müşterisi Profili:** Internet üzerinden, kurumun web servislerine erişilebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. Internet üzerinde kuruma ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
- iii. **Kurumun Misafir Profili:** Kurumu ziyaret eden kişilerin misafir ağında oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
- iv. **Kurumun Çalışanı Profili:** Kurum personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturma amacıyla bu profil kullanılmalıdır. Kurum çalışanı profili ile gerçekleştirilecek testlerde, kurum çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir. Kurum çalışanı profili ile yapılan testlerde, testi yapan kişi/kuruluşa kurum tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilir.

Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

Temel sızma testleri aşağıda tanımlanan sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve açıklık taraması/araştırması tüm bilgi sistemi varlıklarına uygulanır.

- i. **Sistem Tespiti:** Sunucu veya aktif/pasif ağı cihazlarının sistem/yapılardırma bilgilerinin tespit edilmeye çalışıldığı adımdır.
- ii. **Servis Tespiti:** Kurumun bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.
- iii. **Açıklık Taraması/Araştırması:** Kurumun bileşenleri ve bu bileşenlerin sunduğu servislerin açıklık tarayıcıları ile güncel açıklıklara karşı tarandığı ve muhtemel güvenlik açılarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklıklar için açıklär veri tabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

Temel Sızma Testleri

- i. Internet üzerinden gerçek ekleştirecek ek temel sızma testleri: Kurum ağından bağımsız bir lokasyondan, kurumun internet üzerinde sahip olduğu IP ağları taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.
- ii. Kurum iç ağından gerçekleştirilecek temel sızma testleri: Kurumun iç ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:
 - Kurum yerel ağ haritası tespiti
 - Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin yapılması
 - Yerel ağ içerisinde zayıflık taraması yapılması
 - Kurum yerel ağında araya girme teknikleri ile hassas bilgilerin elde edilmeye çalışılması
 - Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırısının yapılması
 - Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşımına çalışılması
- iii. Kurum şube ağında gerçekleştirilecek temel sızma testleri: Kurumun şube ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:
 - Şube yerel ağ haritasının tespiti
 - Şube yerel alan zayıflık taraması yapılması
 - Şube yerel ağında araya girme teknikleri ile hassas bilgilerin elde edilmeye çalışılması
 - Ağ altyapısında bulunan aktif cihazların testlerinin yapılması
 - Şube personelinin bilgisayarı üzerinden oluşturulabilecek tehditlerin incelenmesi
 - Elde edilen bilgiler ışığında şube ağından erişilebilten diğer sunucu ve sistemlere yönelik ele geçirme saldırısının yapılması

SIZMA TESTİ SONUÇLARININ TAKİBİ

Kurumlar, sizme testleri sonucu tespit edilen bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri, tespit edildiği varlıkların değerini ve sizme testi raporlarında yer alan önerileri dikkate alarak, forum yönetim kurallarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip eder. Sizme testleri sonucu ortaya çıkan tespitler, aynı zamanda teftiş kurullarının iç denetim planına da dahil edilir. Bu kapsamda gerek duyulacak hususlara ilişkin ilave açıklamalar Bilgi Güvenliği Yetkilisi 'ne yapılır.

GENEL DURUM VE GELİNEN SON DURUM

Sistem üzerinde gerçekleştirilen Penetrasyon Testi sürecinde sistemin genel mimari yapısı analiz edilir, sunucu yapısı, uygulamalar, iç ve dış kaynaklar incelenir. Sistemin güvenlik kontrolü ihtiyacı belirlenir. Bu analiz ve test süreci bittikten sonra sistem üzerindeki zafiyetlerin kaynakları belirlenmiş olur. Saldırganların gerçekleştirebilecekleri saldırılardır belirlenir, senaryolarla müşteriye aktarılır.

Testlerimiz iki kategoride gerçekleşmektedir. İlk test kategorimiz Dış Test (Black Box) sürecidir. Bu süreçte müşteri firmadan herhangi bir bilgi almadan, tamamıyla bir saldırgan (hacker) bakış açısıyla internetten sistemlerinize erişim gerçekleştirilir. Açıklar ve zafiyetler tespit edilerek, bunların önem dereceleri ve kapatılmasına dair çözümler raporlanır. İkinci kategori İç Test (White Box) sürecidir. Bu aşamada firmadan, sistemler ve ağ yapılandırması hakkında bilgiler alınarak güvenlik uzmanlığımızın firmanın iç ağından erişilebilir olan sunucular üzerinde yaptığı testler gerçekleştirilir. Yine bu test sonucunda da sistem ve ağ üzerindeki açıklar, zafiyetler tespit edilir. Oluşabilecek tehdit senaryoları ile birlikte açık ve zafiyetlerin önem dereceleri, çözüm önerileri raporlanarak firmaya sunulur.

Zafiyetlerin önem dereceleri ve etkileri ile ilgili bilgi verilir. Bu bilgilere göre firmanın zafiyet kapatma ve önlem alma aşamalarında öncelik politikasının belirlenmesinin kolaylaşması amaçlanır. Hazırlanan ve sunulan rapor doğrultusunda açıklıkların/zafiyetlerin kapatılıp gereklili önlemlerin alınması, firmanın sorumluluğundadır.

ZAFİYET TÜRLERİ

Bilgi İfşası: Çeşitli sebeplerden kaynaklanan bu durum sunucuların/cihazların yapısal durumu ve/veya barındırdığı bilgilerin yetkisi olmayan üçüncü şahısların eline geçebilmesine sebep olur.

Yetki Yükseltme: Kullanıcıların kendilerine tanımlanan yetki sınırlarını genişletebilmelerine sebep olan zafiyetlerdir.

Uzaktan Komut Çalıştırma: Saldırganın tampon/yığın bellek taşması vb. diğer yapısal sorunları sömürerek uzak sunucular üzerinde yetki sahibi olmaksızın komut işletmelerine izin veren yüksek dereceli zafiyetlerdir.

ZAFİYET ETKİLERİ

Sistem üzerinde Dış Test ve İç Test olmak üzere iki farklı test süreci gerçekleştirilmiştir. Dış test sürecinde sizlerden firmanızın sistemi ile ilgili herhangi bir bilgi almadan sistemin güvenlik açıklarının bulunması için çalışmalar yapılmıştır.

Dış test sürecinde bulunan zafiyet türlerinin isimlerinden de anlaşılacağı gibi genellikle kullanıcı veya sunucu bilgi ifşalarına yönelik güvenlik açıkları bulunmuştur. Web sitesi üzerinde kullanılmakta olan servislerle ilgili güncelleme eksikliği, sistem güçlendirme eksikliği, konfigürasyon hataları, erişimi kolay basit şifre kullanımı gibi konuların ağırlıklı olduğu zafiyetler keşfedilmiştir. Bu zafiyetler saldırganların bilgi toplama aşamalarını oldukça kolaylaştıracak olan güvenlik açıklarıdır.

Kullanıcı bilgilerinin tespit edilebilirliği, kullanıcı hesapları içinde saldırganların istedikleri değişiklikleri yapabilirliği vb. gerçekleşmesi olası durumlar müşteri, güven ve itibar kaybına yol açar. Aynı şekilde sadece kullanıcıların hesapları ile yetinmeyip, firma sistemine sızabilme ihtimalinin açık olması da firmanızın iş süreçlerini etkileyerek bir tehdit oluşturmaktadır.

Dış test sürecinin bitmesinden sonra sizlerden firmanızın sistemi ile ilgili test sürecinde gerekli olacak bilgilerin alınmasıyla birlikte İç Test süreci başlatılmıştır. Sisteminizin iç yapısı ile ilgili güvenlik açıklarının bulunması için çalışmalar yapılmıştır.

İç Test sürecinde bulunan zafiyetlerin isimlerinden anlaşılacağı gibi Dış Test sürecinde bulunan zafiyetler ile benzerlik gösterdiği görülmektedir. Dış Test sürecinde karşılaştığımız birçok zafiyetin de kaynağı olan İç Test sürecinde bulduğumuz zafiyetler daha tehlikeli durumlarla karşılaşma riski oluşturmaktadır.

Saldırganlar, müşterilerinizin ve firma içi çalışanlarınızın bilgilerini elde edebilirler. Saldırganlar tarafından tüm hesapların (iç/dış müşteri) ele geçirilerek, kontrol edilme riski çok üst düzeydedir. Bununla birlikte saldırganlar sizin sisteminde bulunan gizli verilerin olduğu dosyalara erişim sağlayabilirler ve bu bilgileri çalıp, sizi yanlış yönlendirecek veriler ile değiştirebilirler.

Yukarda bahsettiğimiz zafiyetlerden kaynaklı, firma aleyhine durumlar yaşamamanız için, UITSEC Güvenlik Uzmanları'nın, zafiyetlerin (güvenlik açıklarının) kapatılması doğrultusunda Penetrasyon Testi Raporu içerisinde sundukları çözüm önerilerini dikkate almanızı öneririz.

TEHDİT SENARYOLARI

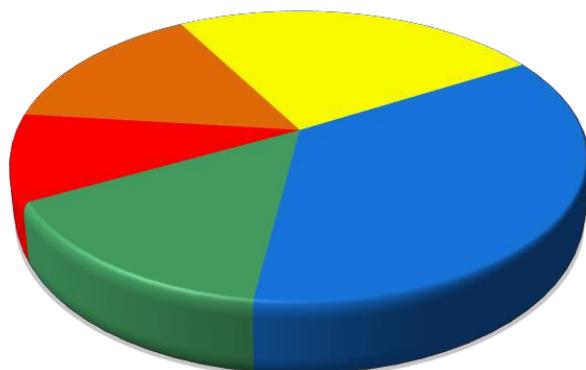
Dış Test ve İç Test süreçlerinde karşılaşılan güvenlik açıkları ile ilgili olası tehditleri aşağıdaki gibi özetleyebiliriz;

- Müşterilerin (iç-dış) hesaplarına erişim sağlanabilir, istenilen değişiklikler yapılabilir ve firma aleyhine yanlış yönlendirmeler gerçekleştirilebilir.
- Erişilebilir bilgiler ile firma vizyon ve misyonunun aksine çalışmalar yapılabilir.
- Sistem içinde kayıtlı bilgilere ulaşılabilir, bu bilgiler çalınabilir ya da zararlı veriler ile değiştirilebilir.
- Online sistem üzerinden firma aleyhine yayınlar yapılabilir, müşterilere yanlış bilgilendirme yapılabilir.
- Müşterilerin güvenleri sarsılır, itibar kaybı oluşur ve toparlanması zor ya da imkansız sonuçlar doğabilir.

ZAFİYET DAĞILIMI

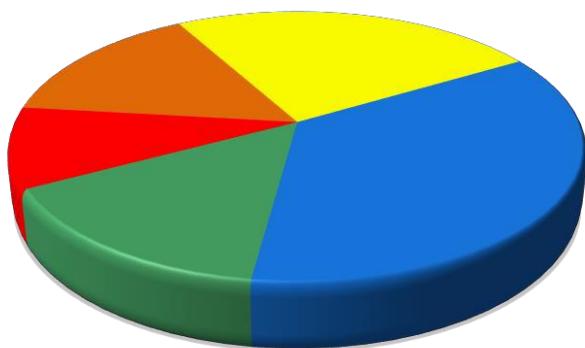
Zafiyetlerin dağılımı testin yapıldığı kurumun yapısına ve sistemine göre değişiklik göstermektedir. Şu zamana kadar gerçekleştirdiğimiz testleri ve bulduğumuz zafiyetlerin tehdit seviyelerini baz alacak olursak, dış test ve iç test süreçleri için zafiyet dağılımlarını aşağıdaki grafiklerde belirttiğimiz gibi özetleyebiliriz.

DIŞ TEST ZAFİYET DAĞILIMI



■ ACİL ■ KRİTİK ■ YÜKSEK ■ ORTA ■ DÜŞÜK

İÇ TEST ZAFİYET DAĞILIMI



■ ACİL ■ KRİTİK ■ YÜKSEK ■ ORTA ■ DÜŞÜK

ZAFİYET SINIFLANDIRMA KRİTERLERİ

| ZAFİYET TEHDİT SEVİYESİ TABLOSU | | UITSEC |
|---------------------------------|---|--------|
| Acil 13 - 15 | Trojan benzeri yazılımlar / Uzaktan komut çalıştırma / Limitsiz dosya erişimi | |
| Kritik 10 - 12 | Saldırganlara uzaktan Root ya da Admin yetkisi verebilen programlar | |
| Yüksek 7 - 9 | Kontrolsüz dosya erişimi / Servis engelleme (DoS) ihtimali | |
| Orta 4 - 6 | Konfigürasyon ya da sunucu dizini vb. hakkında bilgi ifşası | |
| Düşük 1 - 3 | Risk oluşturmayan ama başka vektörlerle birleşerek riske dönüştürülebilecek bilgi | |

SIZMA TESTİ BULGULARI**DIŞ TEST BULGULARI**

| TEHDİT SEVİYESİ | ACİL | |
|---|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.01 | | |
| ZAFİYET ADI | SQL INJECTION | |
| ZAFİYET AÇIKLAMASI | <p>SQL Injection zayıflığı yazılımın veri tabanı ile kurduğu bağlantılarla, kullanıcıdan aldığı parametreleri yeterli düzeyde düzenlememesinden kaynaklanmaktadır. Bu vektör erişim yetkisi ile doğru orantılı olarak yazılım üzerinde bulunan kullanıcının yapabileceği her şeyi saldırganın emrine teslim etmektedir. Saldırgan herhangi bir veriyi ekleyebilir, silebilir, okuyabilir veya değiştirebilir. SQL Injection saldırılarda en kritik nokta kullanıcının yetkilерinde açık bulunan modüllerdir. Gelişmiş veri tabanı sistemleri üzerinde oluşabilecek en kritik zayıflık sistem çağrısının açılması olacaktır (Terminal'e taleplerde bulunulması). MSSQL Yazılımları'na bağlı olarak 'xp_cmdshell' tetikletilebilir ve sunucu problemsiz bir şekilde ele geçirilebilir. Bu işlem iki farklı şekilde uygulanabilir. Birinci yöntem; Administrator grubuna eklenecek yeni bir kullanıcı ile RDP bağlantı alınabilir veya sunucuya yüklenerek çalışılacak özel Scriptler ile sunucunun yönetimi ele geçirilebilir.</p> <p>SQL Injection saldırısı sonucu veri tabanı tiplerine özgü saldırı vektörleri oluşturmaktadır. Ancak genel durum olarak incelediğinde bir SQL Injection zayıflığının sömürülmesi sonucunda saldırgan çok değerli verilere ulaşacaktır. Saldırgan veri tabanından edindiği bilgiler ile Phising saldıruları yapabilir veya sistem üzerinde bulunan CMS'in kullanıcı adı ve şifrelerine, veri tabanı kullanıcı adı ve şifrelerine ulaşabilir, sayfa içeriklerini değiştirerek XSS, RFI gibi saldırıcı teknikleri için uygun altyapıları yerleştirebilir.</p> <p>Saldırganın CMS'e erişebilmesi halinde bu yazılım üzerinde bulunan dosya yükleme scriptlerini kullanarak kendi Backdoorlarını yerleştirebilir ve de cihaza sizerek saldırısına buradan devam edebilir. Sunucuya sizmiş olan saldırgan yazılımın kaynak koduna ekleyeceği görünmeyen bir iFrame sayesinde ziyaretçilerin tarayıcılarının (Browser) zayıflarlarından ziyaretçilerin bilgisayarlarına sizabılır. Sisteme Malware bulaştırılır, Private networkiniz üzerinde bulunan diğer cihazların zayıflarını bularak bunlara sizabılır... Sisteme sizmiş bir saldırganın yapabileceği saldırular bu noktadan sonra teknik bilgisi ve de hayal gücüne kalmaktadır.</p> <p>T- SQL, Oracle gibi birçok veri tabanın Command Shell ile konuşmasını sağlayacağı eklentileri bulunmaktadır, bu eklentilerin açık olduğu noktalarda saldırgan SQL Injection zayıflığı üzerinden sisteme istediği işlemleri yapabilen CMS yazılımıyla ilgilenmeyerek direkt olarak Command Shell'den Backdoor'unu yükleteker çalıştırabilir.</p> <p>MySQL gibi birçok veri tabanı tipinde dosya yükleme opsyonu bulunmaktadır. Bu opsiyon sayesinde SAM dosyası veya Passwd dosyası yükletilerek buradaki kullanıcı adı şifrelerine erişilebilir (tabii ki bu veriler Hash'lenmiş halde bulunacaktır bu yüzden Decrypte edilmeleri gerekmektedir) ve bu şifreler ile uzaktan bağlantı alınabilir ve de daha evvel bahsettiğimiz saldırıcı türlerinin tamamı tekrardan burada uygulanabilir.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ANONİM | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com | |
| ÇÖZÜM ÖNERİSİ VE ALINABILECEK KÖNLEMLER | Kullanıcıdan alınmış her veri öncelikle karakter seti kontrolüne tabi tutulmalıdır. Karakter seti kontrolünden başarıyla geçtikten sonra veri tabanı iletişiminde kullanılan | |

| | |
|-------------|--|
| | <p>kullanmakta olduğu karakter setinin aynı olması gerekmektedir. Kullanıcıdan alınmış veri serialize işlemlerine tabi tutulabilir, bu belirli ölçülerde SQL Injection'ı zorlaştıracaktır.</p> <p>Ancak alınması gereken iki kritik önlem bulunmaktadır. Birincisi; kullanıcıdan alınmış verinin içerisinde tırnakların önüne '\' karakteri koymalıdır. İkincisi; alınmış biri tırnaklar içerisinde SQL Query eklenmesi gerekmektedir.</p> <p>Prosedürel yaklaşımlarınız bulunmaktadırsa, prosedürlerin yazılımsal altyapıları kullanmakta olduğunuz '.net' platform kadar gelişmiş olmadığı için üretilmiş önlemler çoğunlukla atlatılabilirinmektedir. Prosedürsel yaklaşımınızda aşağıda belirtilen kod bloğu yönteminin uygulanmasını tavsiye ederiz. Ancak bu noktada dikkat etmeniz gereken konu kullanıcıdan aldığınız herhangi bir veriye göre SQL Query'niz değişmemelidir. Aksi takdirde daha farklı riskler ile karşı karşıya kalabileceksiniz.</p> |
| REFERANSLAR | <ul style="list-style-type: none"> • https://www.owasp.org/index.php/SQL_Injection • https://www.simple-talk.com/sql/learn-sql-server/sql-injection-defense-in-depth/ |

| TEHDİT SEVİYESİ | ACİL | |
|---------------------------------------|--|---|
| ZAFİYET KODU | CVE | B |
| ZTKD.20141222.02 | | |
| ZAFİYET ADI | KOMPLEX OLMAYAN / VARSAYILAN ŞİFRE KULLANIMI | |
| ZAFİYET AÇIKLAMASI | <p>www.uitsec.com adresinde (dış hosting) barındırılan web uygulamasına yapılan testlerde ele geçen kullanıcı şifreleri arasında sıkılıkla "12345" şifresinin görüldüğü kaydedilmiştir. Bu şifrenin web uygulamasındaki default şifre olduğu ve kullanıcılar tarafından değiştirilmediği tahmin edilmektedir. Bu tip kolay kırılabilir şifrelerin kullanılması uygulama güvenliğini riske sokmaktadır.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski:</p> | |
| KULLANICI PROFİLİ | ANONİM | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLCEK ÖNLEMLER | Karmaşık şifre kullanımı önerilir. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | ACİL | |
|--------------------|---|---|
| ZAFİYET KODU | CVE | B |
| ZTKD.20141224.04 | | |
| ZAFİYET ADI | JBoss ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | <p>JBoss'un yapısında bulunan InkoverServlet üzerinden yapılan dosya upload talepleri normal bir şekilde çalışmış ve sistem üzerinden bize iletişim açmıştır. Bu zafiyetin tetikletilmiş olması, Server'ın dış network ile iç network arasında köprü görevi görmesini sağlamıştır. Sunucuya sızımasından sonra belirli yöntemler ile talepler köprü görevi gören cihaz üzerinden iç networkdeki cihazlara gönderilmiştir.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski:</p> | |

| | |
|--|--|
| KULLANICI PROFİLİ | ANONİM |
| ERİŞİM NOKTASI | INTERNET |
| TESPİT EDİLEN BİLEŞENLER | Konfigürasyon ve Yazılım |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Çıkmış olan en yeni güncelleme versyonunun kullanılması gerekmektedir. |
| REFERANSLAR | |

| TEHDİT SEVİYESİ | ACİL | |
|--|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.06 | | |
| ZAFİYET ADI | XSS ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | <p>Sistemler çalışma esnasında hata alması durumunda IIS konfigürasyonuna bağlı olarak belirli oranlarda bilgi paylaşmaktadır. Sistemlerin paylaştıkları bilgi düzeyi riskin artması ile paralel olarak ilerlemektedir. IIS üzerinde bulunan 'Debug' opsyonu, sunucunun hata alması halinde yazılımın hata almış olduğu kod bloğunu kullanıcıya göndermektedir. Kullanıcı ile bu denli bir bilgi paylaşımı saldırganlar tarafından fark edildiğinde sistemin birçok farklı noktasında hata üretilmesini sağlayarak açık kaynak kodları okuyabilir ve çalışma mimarisi hakkında yorumlarda bulunabilir. Debug Opsyonu'ndan ötürü yazılmış SQL bağlantı String okunabileceği gibi bu durumla testlerde sıklıkla karşılaşılmaktadır.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | MISAFİR | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | <p>Kullanıcıdan alınmış her veri öncelikle karakter seti kontrolüne tabi tutulmalıdır. Karakter seti kontrolünden başarıyla geçtiken sonra veri tabanı iletişiminde kullanılan karakter seti ile sistemin kullanmakta olduğu karakter setinin aynı olması gerekmektedir. Kullanıcıdan alınmış veri serialize işlemlerine tabi tutulabilir, bu belirli ölçülerde SQL Injection'ı zorlaştıracaktır.</p> <p>Ancak alınması gereken iki kritik önlem bulunmaktadır. Birincisi; kullanıcıdan alınmış verinin içerisinde tırnakların önüne '\' karakteri koymalıdır. İkincisi; alınmış veri tırnaklar içerisinde SQL Query eklenmesi gerekmektedir.</p> <p>Prosedürel yaklaşımlarınız bulunmaktadırsa, prosedürlerin yazılımsal altyapıları kullanmakta olduğunuz '.net' platform kadar gelişmiş olmadığı için üretilmiş önlemler çoğunlukla atlatılabilirilmektedir. Prosedürsel yaklaşımlarınıza aşağıda belirtilen kod bloğu yönteminin uygulanmasını tavsiye ederiz. Ancak bu noktada dikkat etmeniz gereken konu kullanıcıdan aldığınız herhangi bir veriye göre SQL Query'niz değişmemelidir. Aksi takdirde daha farklı riskler ile karşı karşıya kalabileceksiniz.</p> | |
| REFERANSLAR | <ul style="list-style-type: none"> https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) | |

| TEHDİT SEVİYESİ | ACİL | |
|--|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.11 | | |
| ZAFİYET ADI | CSRF ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | <p>SRF saldırısı son kullanıcıya servis veren uygulamalar için ileri düzeyde riskli bir vektördür. CSRF zafiyeti kullanıcının girdiği bir sitede, kullanıcının fark etmeden sizin sisteminize taleplerde bulunması sağlanabilir. Bu zafiyet tüm uygulamayı kapsamaktadır, yaptığımız testler esnasında kullanıcı ekleme alanı üzerinden saldırlılar gerçekleştirerek ilerlemiş durumdayız. Saldırı esnasında 50 adet hesap açmış durumdayız, bu noktada bir tek düzenleme gerekmektedir. GET parametresi olarak gönderilen kullanıcının sahip olacağı ID bilgisi POST bilgisinin içinde de bulunması gerekmektedir. Saldırlılar sonucunda hesapların tamamını siteme isletebilmiş bulunmaktadır.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | MISAFİR | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | YAZILIM / LOGOUT HARİC TÜM ALANLAR | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | <p>Session üzerine tamamıyla Random şekilde üretilmiş bir veri hazırlanarak kaydedilip, aynı veri form içeriğine eklenmelidir ve kullanıcından alınan taleplerde içeriklerin birebir aynı olması beklenmelidir ve bir kez kontrol edildikten sonra veri silinerek yeni ürettirilmelidir.</p> | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | KRİTİK | |
|--|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.17 | | |
| ZAFİYET ADI | CAPTCHA ATLATMA | |
| ZAFİYET AÇIKLAMASI | <p>Sistem üzerinde yapılan taleplerde captcha'nın girilmesi zorunlu bırakılmıştır. Captcha üretiltiği esnada veriyi session düzeyinde kayıt altına almaktadır ve gönderilmiş talepte bulunan captcha karşılığı ile kontrol etmektedir. Yazılımın çalışma mantığından her sayfa ürettiğinde captcha bilgisinin tekrardan ürettirileceği ön görülmerek kontrol işleminden sonra sessiondan captcha'nın karşılığı silinmemektedir bu sebepten ötürü talepler tarayıcıdan yapılmadığında (yani aslında görselin adresi talep edilmediğinde) captcha'nın sahip olması gereken değer hiç değişmemektedir. Saldırgan bir defa captcha içeriğini okuyarak tüm alanlardan istediği kadar talepte bulunabilmektedir, session bitiş süresi boyunca herhangi bir doğrulama sürecine tabi olmayacağından.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ANONİM | |
| ERİŞİM NOKTASI | KABLOSUZ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | YAZILIM | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | <p>Kontrol işleminin yapılması ile birlikte captcha'nın açık halinin sessiondan silinmesi gerekmektedir.</p> | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | KRİTİK | |
|---------------------------------------|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.20 | | |
| ZAFİYET ADI | SMTP FLOOD DOS | |
| ZAFİYET AÇIKLAMASI | <p>Kuruluş alt yapılarında bulunan ve kullanıcılarla kendi hesapları ile giriş yapabilmesini sağlayan iki sistem bulunmaktadır, kuruluş işlemlerini yürütebilmesini sağlamak adına e-kuruluş uygulaması ve de bilet satışlarını, etkinlik duyurularını yapmak adına bilet uygulaması zafiyetin tespit edildiği uygulamalardır. Zafiyetin ortaya çıkışının aslı sebebi kullanıcının yaptığı talep sonucunda her seferinde e-posta gönderimi yapan alanların SMTP üzerindeki yetkileri doğrultusunda yaptığı mail gönderimidir. Herhangi biri doğru bilgiler ile yaptığı çok yüksek e-posta gönderim talebi sonucunda SMTP servisi kesintiye uğrayacaktır. Bu noktada bağlantıyı yavaşlatmak adına domain'in bilgisini barındıran DNS servisinin daha yavaş cevap vermesi sağlanabilir veya SMTP servisinin (kullanıcı hesabının üzerinde bulunduğu) daha yavaş cevap vermesi sağlanarak paralel işleme tabi tutulan gönderim adedi yükseltilmeli.</p> | |
| ZAFİYETİN ETKİSİ | SERVİS DURDURMA | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ANONİM | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com/SifremiUnuttum | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLCEK ÖNLEMLER | <p>Otomatikleştirilmesi halinde belirli bir noktadan sonra e-posta gönderimi durdurulmalıdır, şifre sıfırlama alanı olmasından ötürü 3 kere e-posta gönderildiğinde e-posta gönderimi engellenerek kullanıcıya gönderilmiş linklerden birinin kullanılması gerektiği söylenebilir. Bu noktada açık metin şifre saklama zafiyeti raporlanmış olduğu için kullanıcıya açık metin şifresi gönderilemeyecektir ve şifre sıfırlama alanı yaratılması gerekecektir bu yüzden link olarak ifade edilmiştir.</p> | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | KRİTİK | |
|---------------------------------------|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.27 | | |
| ZAFİYET ADI | DIRECTORY LISTING | |
| ZAFİYET AÇIKLAMASI | <p>Bu zafiyet uzun zamanдан beri etkin olan ve saldırganların bilgi ifşası noktasında en çok sömürdüğü zafiyelerden biridir. Web sunucular olabildiğince gizli kalmaya ihtiyaç duyarlar. Ancak DirectoryListing açık olması halinde dosya içeriklerinin tamamı kullanıcıya bildirilmektedir. Bu durumdan ötürü yüklenmiş her türlü dosya saldırganlar tarafından kolaylıkla tespit edilerek yüklenebilecektir. Bu tip bir durum yalnızca yüklenmiş bir dosyanın bilgi ifşasıyla kalmamaktadır, içerisindeki yazılımlar hakkında doküman veya exe'lerin barındırılması da ayrı bir zafiyet haline gelmektedir. Çünkü spesifik görevler için hangi uygulamaların kullanılmakta olduğu ortaya çıkmaktadır.</p> | |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | MÜŞTERİ | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com/en/notes/ | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLCEK ÖNLEMLER | Mevcut Directory Listing kapatılmalıdır. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | YÜKSEK | |
|--|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.43 | | |
| ZAFİYET ADI | MCRS AĞI YETERSİZ GÜVENLİK ÖNLEMLERİ | |
| ZAFİYET AÇIKLAMASI | Bu ağ çalışma yapısı olarak yanlışca MAC adresini kontrol ederek çalışmaktadır. Ortam yapısı itibarıyle kullanıcılar dağıtıclara uzak oluşu, wpa/wpa2 ailesi olmasından ötürü kırılması muhtemel handshake bulunmakta, bu da herhangi bir kullanıcının bağlantısının hacklenmesi sonucunda tüm ağın gizliliğini etkileyecektir. Çalışmalar esnasında birkaç dakika içinde handshake paketi yakalanmıştır. | |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | KONFIGÜRASYON | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | WPA2 enterprise kullanarak kişiye özgü şifreler kullanılabilir ancak en sağlıklı ve etkili çözüm olarak hotspot kullanmanızı öneririz. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | YÜKSEK | |
|--|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.44 | | |
| ZAFİYET ADI | SIRIXMOBILE HTTP PROTOKOLÜ ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | Mobil trade uygulaması olan sirixmobile uygulaması web sayfasını sirixmobile.uitsec.com.tr adresinde yayılmışmaktadır bu uygulama mobilde çalışmak için hazırlanmıştır ve de https protokolünü desteklememektedir, https protokolü ile yapılan erişimlerde flash olan uygulama açılmaktadır. Bu durum HTTP protokolünün zayıflıklarının tamamını ortaya çıkarmak ile birlikte mobil cihazların paylaşımı wireless ağlarına sıkça bağlandığı düşünüldüğünde risk seviyesi yüksek bir durum haline gelmektedir. | |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | MÜŞTERİ | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | http://sirixmobile.uitsec.com.tr | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Uygulamanın tamamının HTTPS trafiği ile iletişimini gerçekleştirdiğinden emin olunması gerekmektedir. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | YÜKSEK | |
|--------------------|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.48 | | |
| ZAFİYET ADI | KULLANICI İSMİ TESPİTİ | |
| ZAFİYET AÇIKLAMASI | Firma subdomaininde bulunan EBA uygulaması üzerinden kullanıcı hesapları tespit ettilerilebilinmektedir. Kullanıcı giriş alanında Username olarak bulunan bir hesap verildiğinde kullanıcı adına bağlantı alınmadı uyarısı verilmekte iken olmayan bir kullanıcı adı kullanıldığı durumlarda | |

| | |
|--|---|
| | geçersiz kullanıcı olarak uyarı vermektedir. Bu durum saldırganların kayıtlı kullanıcıları tespit edebilmesini sağlayacaktır ve yapılması muhtemel Brute Force saldırılarda kullanıcı isminin bilinmeyen olduğu etkili olacaktır. |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: |
| KULLANICI PROFİLİ | ANONİM |
| ERİŞİM NOKTASI | INTERNET |
| TESPİT EDİLEN BİLEŞENLER | eba5.uitsec.com.tr |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Hesap isimleri bulunması ya da bulunmaması durumunda verilen uyarılar aynı olmalıdır. |
| REFERANSLAR | |

| TEHDİT SEVİYESİ | ORTA | |
|--|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.80 | | |
| ZAFİYET ADI | URL YAPISI DÜZENLEME HATASI | |
| ZAFİYET AÇIKLAMASI | <p>URL yapıları uygulamaların çalışma mantıkları, dosya/doküman konuşturma formatları gibi bazı bilgileri paylaşmaktadır. Bir uygulamanın altyapısında bulunan uygulamanın tespiti gibi sonuçlar doğurabileceği gibi özelleştirilmiş kullanıcılara ayrılmış alanlar hakkında bilgi veriyor olması saldırgan için saldırıyı başlatacağı noktanın belirlenmesine sebebiyet verecektir. Sistemin hata aldığı noktalarda /uitsec/admin/ adresine yönlendirmesi sistem yönetiminin '/admin/' uzantısından sonra gelecek bir kısım ile sağlanacağını göstermektedir.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ANONİM | |
| ERİŞİM NOKTASI | INTERNET | |
| TESPİT EDİLEN BİLEŞENLER | YAZILIM | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Dosyalamadaki uzantıdan admin kısmının kaldırılması en sağlıklı olacaktır. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | ORTA | |
|--------------------|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKD.20141222.82 | | |
| ZAFİYET ADI | DNS YAPILANDIRMA HATASI (SFTP) | |
| ZAFİYET AÇIKLAMASI | <p>DNS altyapısı insan zekasına daha uygun olan alfabetik tanımlama sistemi sayesinde günümüzde internet ağında ana yönlendirici omurga halini almıştır. Bu servis firmaların dış ağlardaki, iç ağlardaki varlıklarının tespitinde öncül bir kaynak olarak kullanılmaktadır bu yüzden tahmin edilebilir domain isimleri veya fazla bilgi içeren domain isimleri de sistemler hakkında bilgi paylaşabilmektedir. DNS (NS) veya posta (MX) servisleri DNS üzerinde zaten kayıtlı olmak zorunda olan içerikler olmalarından ötürü bu zafiyet onları kapsamamaktadır ancak 'sftp', 'crm' Subdomainleri yapının gözlemlenebilmesinde ve tespitinde büyük rol oynamaktadır. SFTP servisi FTP Over SSH olarak değerlendirileceğinden ötürü sunucu üzerinde SSH servisi bulunduğu bilgisi paylaşmaktadır buda saldırganların direkt olarak o porta yönetebilmelerini sağlamaktadır. Firewall konfigürasyonunda bulunan port tarama önlemi genel yapıda yapılan port taramalarını tespit edip koruma sağlamaktadır ancak kullanıcının CRM</p> | |

| | |
|--|--|
| | uygulamasının nerede barındırıldığını öngörebilmesi veya SFTP servisinin öngörülebilmesi yapı analizinde bilgi ifşasına sebebiyet vermektedir. |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: |
| KULLANICI PROFİLİ | ANONİM |
| ERİŞİM NOKTASI | INTERNET |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com |
| ÇÖZÜM ÖNERİSİ VE ALINABILECEK ÖNLEMLER | Daha az bilgi veren isimler tercih edilmelidir. |
| REFERANSLAR | |

| TEHDİT SEVİYESİ | DÜŞÜK | |
|--|--|-----|
| ZAFİYET KODU | CVE | BİD |
| ZTKD.20141222.106 | | |
| ZAFİYET ADI | ADMIN ADRESİ TESPİTİ | |
| ZAFİYET AÇIKLAMASI | Ana domain olan uitsec.com.tr adresinde çalışmalarımız esnasında birçok dizin tespit edilebilmiş bulunmaktadır ancak yönetim panelinin giriş adresi tespit edilememiştir. Uygulamanın erişim adresinin tespit edilememiş olması ile birlikte 'admin' dizininin olduğu gözlemlenmektedir. Bu dizin direkt olarak uygulamayı yönetmek için hazırlanmış uygulamanın içeriklerinin bu dizinde tutuldu düşülmektedir. | |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ANONİM | |
| ERİŞİM NOKTASI | KABLOSUZ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | www.uitsec.com/admin | |
| ÇÖZÜM ÖNERİSİ VE ALINABILECEK ÖNLEMLER | Dizin isminin değiştirilmesi ve tahmin edilmesi güç bir isim seçilmesi önerilir, mümkün ise yönetim arayüzünün yalnızca iç ağ üzerinden erişilebilir oluşu tercih edilmelidir. | |
| REFERANSLAR | | |

İÇ TEST BULGULARI

| TEHDİT SEVİYESİ | ACİL | |
|--|--|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.01 | CVE-2009-2526, CVE-2009-2532, CVE-2009- 3103 | 36299 |
| ZAFİYET ADI | MICROSOFT WINDOWS SMB2 NEGOTIATION PROTOCOL REMOTE CODE EXECUTION | |
| ZAFİYET AÇIKLAMASI | MS09-050 güncellemesinin eksikliğinden dolayı mevcut olarak tetiklenen bu zayıfet ile saldırgan özel hazırlanmış SMB version 2 paketleri ile yaptığı saldırılarda başarılı olması durumunda sistem düzeyinde yetki sahibi olmuş olur, başarısız olan saldırılarda ise servisi durdurma noktasına rahatlıkla getirebilir. | |
| ZAFİYETİN ETKİSİ | SERVİS DURDURMA | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 10.100.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABILECEK ÖNLEMLER | Aşağıdaki linkte verilen mevcut MS09-050 güncellemesinin uygulanması gerekmektedir. http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | ACİL | |
|--|---|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.02 | CVE-2008-4114, CVE-2008-4834, CVE-2008-4835 | 31179 |
| ZAFİYET ADI | MS09-001 | |
| ZAFİYET AÇIKLAMASI | Yapılan araştırmalarda sunucu/cihazlar üzerinde MS09-001 güncellemesinin eksik olduğu tespit edilmiştir. Zayıfetin temeli Server Message Block(SMB) protokolünün kendisine gelen özel hazırlanmış SMB paketlerini işleme sokmasından gelmektedir. Başarılı saldırı sonrası yetkisiz saldırganlar servisin durmasına yol açabiliirlر. | |
| ZAFİYETİN ETKİSİ | UZAKTAN KOMUT ÇALIŞTIRMA | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 192.168.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABILECEK ÖNLEMLER | Sorunun çözümü için Windows Update ile veya manuel bir şekilde gerekli güncelleştirme yüklenmelidir. Aşağıdaki link'den mevcut güncelleştirme ve güncelleştirme hakkında detaylı bilgilere ulaşılabilir. http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx | |
| REFERANSLAR | http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx | |

| TEHDİT SEVİYESİ | ACİL | |
|--|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.06 | | |
| ZAFİYET ADI | SSH / FTP DEFAULT KOMBİNASYON İLE ERİŞİM | |
| ZAFİYET AÇIKLAMASI | <p>Kullanmakta olduğunuz çeşitli servislerin sunucularının incelenmesi ve ilk aşamalara dahil olan Default/basit Password incelemeleri sırasında aşağıdaki noktalarda basit/Default Password'lara erişilmişdir. Bu noktalarda bulunan sunucularda kullanılmakta olan servislerin Log'ları ve Backup'larına erişilebilmektedir, hızlı erişim ve saldırganın bu noktalardan ağa yayılma hızı da hesaba katıldığından acil olarak değiştirilmesi gerekmektedir.</p> <p>ftp 172.16.0.00 administrator password ssh 172.19.0.00 root letacla</p> | |
| ZAFİYETİN ETKİSİ | YETERSİZ ŞİFRELEME SONUCU ERİŞİM | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 172.16.0.00 / 172.19.0.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Servislerde kullanılmakta olan şifrelerin değiştirilmesi, en az Alphanumeric bir şekilde 8 haneye kadar ulaşan kombinasyonlar ile şifre üretilmesi önerilir. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | ACİL | |
|--|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.007 | | |
| ZAFİYET ADI | MICROSOFT REMOTE DESKTOP PROTOCOL SERVİS DURDURMA ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | <p>Microsoft işletim sisteminde bulunan ve 3389 portunda çalışan RDP servisi kernel seviyesinde çalışıp, uzak masaüstü işlemlerini gerçekleştirmek amacıyla geliştirilmiş bir servistir. Servis iletişim aşamasında aldığı "ConnectMCSPDU" paketini yönetirken "maxChannellds" alanı üzerinde yetersiz denetim kurmasından ötürü servis kesintisi zayıflığı ortaya çıkmaktadır. Zayıflığın tetiklenmesi kullanıcının çıkış esnasında alınan RDPWD!NM_Disconnect bilgisi yanlış referans adresi dönmesiyle başlamaktadır. "MaxChannellds" bilgisi için gönderilecek "\x02\x01\xff" içeriği ile birlikte gönderilen shellcode'lar sunucuları servis veremez hale getirecektir.</p> | |
| ZAFİYETİN ETKİSİ | SERVİS DURDURMA | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 10.100.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | <p>http://technet.microsoft.com/en-us/security/bulletin/MS10-012 adresinden de ulaşabileceğiniz ilgili güvenlik yamalarını yüklemeniz önerilir.</p> | |
| REFERANSLAR | <ul style="list-style-type: none"> • http://blog.binaryninjas.org/?p=58 • http://secunia.com/advisories/48395 • http://support.microsoft.com/kb/2671387 • http://www.securitytracker.com/id/1026790 • http://technet.microsoft.com/en-us/security/bulletin/ms12-020 | |

| TEHDİT SEVİYESİ | KRİTİK | |
|--|--|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.09 | | |
| ZAFİYET ADI | FTP NULL PASSWORD | |
| ZAFİYET AÇIKLAMASI | <p>Yapılan incelemeler sırasında Administrator için şifresiz erişim olduğu tespit edilmiştir. Bu durum enfekte edilmiş dosyaları yerleştirmek için ve diğer saldırılara ön adım olabilecek bilgileri toplamak için sömürülebilir. Saldırgan böyle bir zafiyet ile karşılaşlığında FTP'ye yükleyeceği bir yük dosyasıyla (payload) sistemde yetkisiz bir kullanıcı olabilir. Yetkisiz kullanıcı olan saldırıcı yerel yetki yükseltme betiği (exploit) ile sisteme yetkisi olan bir kullanıcının yetkilerini çalabilir. Bu senaryo dışında diğer kullanıcılar ile etkileşimde olan bir klasöre insanların ilgisini çekecek bir isim ile yük dosyası (payload) yerleştirir. Yük dosyasını indirip incelemek isteyen kullanıcılar istemsiz şekilde saldırının bilgisayarına bağlantı talebi göndererek bilgisayarlarını saldırana açabilirler.</p> | |
| ZAFİYETİN ETKİSİ | UZAKTAN KOMUT ÇALIŞTIRMA | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ Ağ | |
| TESPİT EDİLEN BİLEŞENLER | 10.13.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | FTP hesaplarında bulunan temel kullanıcı hesapları silinmeli, anonim kullanıcıların izinleri konfigürasyonlar ile kaldırılmalı. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | KRİTİK | |
|--|---|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.11 | CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825, CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-2008-4107 | 26403 |
| ZAFİYET ADI | PHP ÇOKLU ZAFİYETLER GRUBU | |
| ZAFİYET AÇIKLAMASI | <p>PHP versiyonlarından kaynaklı toplu zafiyet grubu aşağıdaki gibi verilmiştir. Bunların arasında:</p> <ul style="list-style-type: none"> -Sessions Subsystem Session Fixation Vulnerability -SSL Certificate Validation Security Bypass Vulnerability -Denial Of Service Vulnerability | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | YETKISİZ Ağ İSTEMCİSİ | |
| ERİŞİM NOKTASI | İç Ağ | |
| TESPİT EDİLEN BİLEŞENLER | 10.1.00.00 / 10.101.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Kullanılan servisin güncel stabil PHP sürümü olan 5.5.9 sürümüyle değiştirilmesi önerilir. | |
| REFERANSLAR | <ul style="list-style-type: none"> • http://www.osvdb.org/96316 • http://secunia.com/advisories/54562 • http://cxsecurity.com/cveshow/CVE-2011-4718 | |

| TEHDİT SEVİYESİ | KRİTİK | |
|--|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.12 | CVE-2012-0121, CVE-2012-0122 CVE-2012-0123, CVE-2012-0124 | |
| ZAFİYET ADI | HP DATA PROTECTOR EXPRESS | |
| ZAFİYETAÇIKLAMASI | <p>Belirtilen IPler üzerinde bulunan sunucu/cihazlarda kullanılan HP Data Protector Express sürümü üretici tarafından açıklanan fakat detaylandırılmış uzaktan komut çalışma zafiyetine sahiptir. Başarılı saldırılar uzak sunucu üzerinde kötü amaçlı kod bloklarının çalıştırılabilmesiyle, başarısız saldırılar ise servisin /sunucunun çökmesiyle sonuçlanacaktır.</p> <p>Etkilenen sürümler:</p> <ul style="list-style-type: none"> • HP Data Protector Express 6.0.01 0 • HP Data Protector Express 6.0.00 0 • HP Data Protector Express 5.0.01 0 • HP Data Protector Express 5.0.00 0 <p>Etkilenmeyen Sürümler:</p> <ul style="list-style-type: none"> • HP Data Protector Express 6.0.01 build 13958 0 • HP Data Protector Express 6.0.00 build 11974 0 • HP Data Protector Express 5.0.01 build 70262 0 • HP Data Protector Express 5.0.00 build 59287 0 <p>*Servisin/ugulamanın kullanımının sonlandırılacağı bildirildiği için çözüm önerisi geliştirilmemiştir.</p> | |
| ZAFİYETİN ETKİSİ | | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | YETKISİZ AĞ İSTEMCİSİ | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 10.174.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABILECEK ÖNLEMLER | | |
| REFERANSLAR | <ul style="list-style-type: none"> • http://www.securityfocus.com/archive/1/521944 | |

| TEHDİT SEVİYESİ | YÜKSEK | |
|-------------------|--|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.20 | CVE-2014- | 70574 |
| ZAFİYET ADI | SSLv3 POODLE ZAAFİYETİ | |
| ZAFİYETAÇIKLAMASI | <p>SSL 3.0 versiyonun da bulunan bu zafiyet, sunucuların MitM saldırılarına maruz kalmasına sebebiyet verebilir.</p> <p>SSL 3.0 çözülmüş mesajları şifreleme esnasında Padding Byte'ları işlerken Cipher Block Chaining (CBC) Modu'nu kullanmaktadır. CBC'nin yapısını oluşturan algoritmanın zayıflığından dolayı, şifreleme esnasında kullanılan Padding Byte'lar tahmin edilebilir ve şifrelenmiş trafik çözülebilir. Bunun sonucu olarak saldırgan sunucular üzerinde MitM yaparak normalde şifrelenmiş olarak iletilmesi gereken kritik verileri elde edebilir.</p> | |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI | |
| ZAFİYET RİSKLERİ | <p>İş Riski: BT Riski:</p> | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |

| | |
|---|--|
| TESPİT EDİLEN BİLEŞENLER | 172.30.00.00 |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Zaafiyete sebebiyet veren hata omurgasal olduğundan POODLE için yayınlanmış bir yama henüz bulunmamaktadır. SSLv3 gibi eski protokollerin sunucular üzerinde devre dışı bırakılarak, daha güvenli olan TLS protokülünün kullanılması zaafiyetin giderilmesi için |
| REFERANSLAR | <ul style="list-style-type: none"> • https://www.openssl.org/~bodo/ssl-poodle.pdf • http://www.securityfocus.com/bid/70574/info |

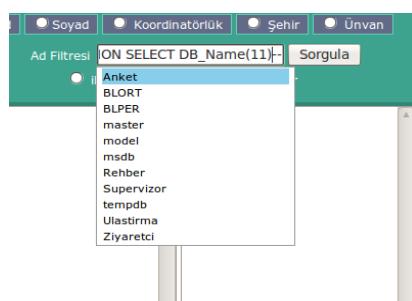
| TEHDİT SEVİYESİ | YÜKSEK | |
|---|---|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.22 | CVE-2009-2526, CVE-2009-2532, CVE-2009-3103 | 36299 |
| ZAFİYET ADI | MICROSOFT SERVER MESSAGE BLOCK ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | MS09-050 güncellemesinin eksikliğinden dolayı mevcut olarak tetkilenen bu zafiyet ile saldırılan özel hazırlanmış SMB version 2 paketleri ile yaptığı saldırırlarda başarılı olması durumunda sistem düzeyinde yetki sahibi olmuş olur, başarısız olan saldırırlarda ise servisi durdurma noktasına rahatlıkla getirebilir. | |
| ZAFİYETİN ETKİSİ | BİLGİ İFŞASI | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 192.168.00.00 / 172.23.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Aşağıdaki linkte verilen mevcut MS09-050 güncellemesinin uygulanması gerekmektedir. http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx | |
| REFERANSLAR | http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx | |

| TEHDİT SEVİYESİ | YÜKSEK | |
|---|---|-----|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.24 | | |
| ZAFİYET ADI | YETERSİZ ŞİFRE POLİTİKA VE PROSEDÜRLERİ | |
| ZAFİYET AÇIKLAMASI | İç testler sonucunda, sunucu ve kullanıcı cihazlarında "Local Administrator" hesaplarında ve email hesaplarında yaygın olarak "Xxxmmm34" şifresinin kullanıldığı saptanmıştır. Kurum genelinde bir şifrenin birden çok noktada yaygın olarak kullanılması bu cihazlardan birinin dahi bilgi ifşası zafiyeti göstermesi durumunda aynı şifrenin kullanıldığı diğer sunucuları ve cihazları riske atacak ve bilgi güvenliği üzerinde domino etkisi yaratacaktır. Buna ek olarak bilgi işlem departmanın yaptığı bilgilendirmeler doğrultusunda şifre yönetimi ve "account lockdown policy"lerin olası Brute Force saldırılarının önüne geçmek konusunda yetersiz kalabileceği kaydedilmiştir. | |
| ZAFİYETİN ETKİSİ | SERVİS DURDURMA VE KESİNTİYE UĞRATMA | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | İÇ AĞ İSTEMCİSİ | |
| ERİŞİM NOKTASI | KURUM İÇİ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK ÖNLEMLER | Karmaşık şifre kullanımının, belirli periyodlar ile (örn: 6 ay) şifre yenilemenin, ilk kullanım şifrelerinin zorunlu değişiminin mecburi kılınması ve kullanıcılara bilgilendirme eğitimi yapılması önerilir. | |
| REFERANSLAR | | |

| TEHDİT SEVİYESİ | ORTA | |
|-------------------------------|--|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.37 | CVE-2009-3294 | 36449 |
| ZAFİYET ADI | PHP ALTYAPI SCRIPTİ KAYNAKLI SERVİS KESİNTİSİ | |
| ZAFİYET AÇIKLAMASI | PHP altyapısında bulunan TSRM dosyasının içindeki tsrm_win32.c scripti Windows işletim sistemi operasyonlarında bulunurken bir hata ile karşılaşmaktadır, bu hata kaynak tüketimini yükselterek servis reddine sebebiyet verebilir. Script üzerinde bulunan API fonksiyonu işlemler esnasında _fdopen fonksiyonunu kullanmaktadır ve bu fonksiyon hata alınmasına sebebiyet vermektedir. | |
| ZAFİYETİN ETKİSİ | SERVİS DURDURMA | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | YAZILIM / 172.16.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK | IIS'in eklentisinin geçersiz kılınması veya servisin IIS 8 sürümüne yükseltilmesi gerekmektedir. | |
| REFERANSLAR | <ul style="list-style-type: none"> • http://en.securitylab.ru/nvd/383831.php • http://downloads.securityfocus.com/vulnerabilities/exploits/31064.php | |

| TEHDİT SEVİYESİ | ORTA | |
|-------------------------------|---|-------|
| ZAFİYET KODU | CVE | BID |
| ZTKI.20141222.40 | CVE-2009-1535 | 34993 |
| ZAFİYET ADI | MICROSOFT ISS WEBDAV REMOTE AUTHENTICATION BYPASS ZAFİYETİ | |
| ZAFİYET AÇIKLAMASI | WebDAV üzerindeki adres düzenleme yapılarından kaynaklı güvenlik atlatma zafiyeti bulunmaktadır. Adres düzenleme sisteminin Unicode değerler üzerindeki düzenlemeler esnásındaki yetersizliği şifre koru mali dosyalara erişim izni sağlamaktadır. Saldırgan bu zafiyeti sömürerek ulaşmaması/ulaşamaması gereken dosyalara ulaşarak bilgi toplayabilir veya saldırular düzenleyebilir. Versiyon kaynaklı zafiyetin geçerliliği tespit edilse de tarafımızca test sürecinde dosya erişimi sağlanmamıştır, özellikle /reports dosyasına erişime çalışılmıştır. | |
| ZAFİYETİN ETKİSİ | YETKİSİZ ERİŞİM | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | |
| KULLANICI PROFİLİ | ÇALIŞAN | |
| ERİŞİM NOKTASI | İÇ AĞ | |
| TESPİT EDİLEN BİLEŞENLER | 172.16.00.00 | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLECEK | IIS'in eklentisinin geçersiz kılınması veya servisin IIS 8 sürümüne yükseltilmesi gerekmektedir. | |
| REFERANSLAR | <ul style="list-style-type: none"> • http://view.samuraijdata.se/psview.php?id=023287d6&page=2 • http://www.microsoft.com/technet/security/advisory/971492.mspx • http://blog.zoller.lu/2009/05/iis-6-webdac-auth-bypass-and-data.html • http://downloads.securityfocus.com/vulnerabilities/exploits/34993.rb • http://downloads.securityfocus.com/vulnerabilities/exploits/34993.txt | |

| TEHDİT SEVİYESİ | DÜŞÜK | | | | |
|---------------------------------------|---|------|--|--|--|
| ZAFİYET KODU | CVE | BİD | | | |
| ZTKI.20141222.63 | CVE-2002-1123 | 5411 | | | |
| ZAFİYET ADI | MICROSOFT'S SQL | | | | |
| ZAFİYET AÇIKLAMASI | Microsoft SQL sunucuların 2005 ve öncesi bazı sürümleri kullanıcı doğrulama adımındaki girdi doğrulama mekanizmasının zayıfyetinden tampon bellek taşması yoluyla sisteme sızmasına, hemen hemen hepsi Brute Force şifre denemesine izin vermektedir. Gene MSSQL serverlarda bulunan "xp_cmdshell stok" prosedürü her ne kadar 2008 ve sonrası sürümlerde kullanıma kapalı halde gelse de sorgularla aktive edilebilmekte ve dışarıdan komut çalıştırılmaya izin vermektedir. Bu zayıflıkları kullanan biri MSSQL sunucunun önce şifresini bulabilir, sonrasında da amacına yönelik olarak sistemde bir dizi komutları çalıştırarak sistemi ele geçirebilir, servisin ya da sunucunun hizmet veremez hale gelmesine sebep olabilir. | | | | |
| ZAFİYETİN ETKİSİ | | | | | |
| ZAFİYET RİSKLERİ | İş Riski: BT Riski: | | | | |
| KULLANICI PROFİLİ | YETKISİZ AĞ İSTEMCİSİ | | | | |
| ERİŞİM NOKTASI | KURUM İÇİ AĞ | | | | |
| TESPİT EDİLEN BİLEŞENLER | 10.174.00.00 | | | | |
| ÇÖZÜM ÖNERİSİ VE ALINABİLİR KÖNLİMLER | <ul style="list-style-type: none"> Microsoft SQL sunucularının aynı ip üzerinden 5--- 10(ya da sizin belirleyeceğiniz tolerans limiti) hatalı denemeden sonra istek gelen Host'u bloklaması Zayıfetin varlığından şüphelenmesini engellemek için 1433 Portlarının filtrelenmesi Servisin standart olan 1433 portu yerine farklı bir port üzerinden çalıştırılması Sadece ön tanımlı adresler üzerinden sunucuya iletişim kurulmasına izin verilmesi Kullanılan portun güvenliğinin firewall ile sağlanması Default "sa" kullanıcısının işlevsiz kılınması Uzun ve karmaşık şifrelerin tercih edilmesi Kullanımda olmayan servisin durdurulması Dışarıdan bağlantı Kabul etmesi gerekmeyen sunucularda portun kapatılması yada filtrelenmesi İşlemlerinden birkaçı ya da tamamı uygulanarak ve kritik yamaların eksiksiz uygulanmasıyla güvenlik sağlanabilir. | | | | |
| REFERANSLAR | <ul style="list-style-type: none"> IAVA:2002-B- 0007 | | | | |

SIZMA KANITLARI**DIŞ PENETRASYON TESTİ SIZMA KANITLARI**SQL Injection Zayıfeti

XSS Zafiyetinin Tetikletilmesi

```
1406 logToConsole("disconnected...");  
1407 },  
1408 onError:function () {  
1409     logToConsole("error...");  
1410 },  
1411 onReceive:function (message) {  
1412     var text = message.data.info;  
1413     var scope = message.data.scope;  
1414     var type = message.data.type;  
1415     var includeHeader = message.data.header;  
1416     if (!text) return;  
1417     if (scope == 'public') {  
1418         var data = $jq.evalJSON(text);  
1419         switch (type) {  
1420             case 1:  
1421                 logToConsole("receiving quote...");  
1422                 if ("private_Watch_List" == "") {}  
1423             //  
1424             alert("XSS DENEME")  
1425         }  
1426     ) {  
1427         if ($jq("table.resultstable tbody tr").len  
1428             updateMarketWatch(data, includeHeader);  
1429         )  
1430     } else {  
1431         updateMarketWatch(data, includeHeader);  
1432     }  
1433     break;  
1434     case 5:  
1435         updateMarketStatus(data);  
1436         logToConsole("receiving market status...");  
1437         break;  
1438     case 9:  
1439         logToConsole("receiving index status...");  
1440         updateIndexData(message);  
1441     }  
1442 }
```



XSS (Cross Site Scripting)

Bilgilendirme: XSS zayıfeti sömürülerek sayfa geçici veya yarı kalıcı (ziyaretçinin cache bellek süresi ile sınırlı) şekilde bozunuya uğratılabilir. Bu sayede ziyaretçiler yamalıtlılar, zombileştirilebilir, ziyaretçilerin bilgilerini çalımlıbir hatta sahte içerik yerleştirebilir firma itibarı ve güvenilirliğini tehdit edilebilir. XSS zayıfetleri aynı zamanda öngörülemeyecek daha birçok saldırvı atmak vektörü olabilmektedir.

Bu imaj sadice önekleme ve bilgilendirme amacıyla UTSEC Firması tarafından hazırlanmış olup UTSEC firmasının yazılı izni olmaksızın kullanılamamıştır. Önekleminin yapıldığı tarihte UTSEC firmasından hizmet almıyor seniz ve mesaiyi phóyal olsanızda dikkatli olun. Duyuruya ulaşın info@utsec.com adresi üzerinden UTSEC ile irtibat kurunuz ve aynı hizmetin size ultiplar dosya ve linklerin kesinlikle egratayınız. Izinli kullanım sonucu olabileceği olası zarardan Sirketimiz (utsec, Universal IT Security Consulting) sorumlu tutulacaktır.



XSS (Cross Site Scripting)

Bilgilendirme: XSS zayıfeti sömürülererek sayfa geçici veya yarı kalıcı (ziyaretçinin cache bellek süresi ile sınırlı) şekilde bozuntuya uğratılabilir. Bu sayede ziyaretçiler yarınlabilir, zombileşirler gibi, ziyaretçilerin bilgilerini çalımlıbir hatta sahte içerik yerleştirerek firma itibarı ve güvenilirliğini tehdit edilebilir. XSS zayıfetleri aynı zamanda öngörülemeyecek daha birçok saldırvı atacak vektörler olabilmektedir.

Bu mesaj sadece örmekleme ve bilgilendirme amacıyla UFTSEC Firması tarafından hazırlanan olup UFTSEC firmasının yazılı ieri olursakta kullanan yasaklı. Örenmekleme yapıldığı tarihte UFTSEC firmasından hizmet almayan, menzil ve mesyan şartının oldugu durumda yorumlanır. Lütfen info@uftsec.com adresi üzerinden UFTSEC ile irtibat kurunuz ve aynı hizmetin söz konusu olduğu tarihe tekrar kesinlikle eylemzeyin. Lütfen kullanım sonucu okunabilecek olası zararlarından Sinkelimit (tutucu, Universal IT Security Consulting) sorumlu tutuluruz.



XSS (

Bilgilendirme: XSS zaf yaretçinin cache bellek sayede ziyaretçiler yançalınabilir hatta sahte içedilebilir. XSS zafliyet saldırısına atak vektörü olur.

Bu imḡ sadece örn̄ekleme ve bilgilendirme
kullanımı yasaktır. Örn̄eklenenin yapıldı
düşünüyorsanız lütfen info@ultsec.com
kesinlikle açmamınız. İzinsiz kullanım sonucu
ütükləməz.

Riskli HTTP Methodları

```
OPTIONS / HTTP/1.0

HTTP/1.1 200 OK
Server: dws/1.2.6-1
Date: Mon, 06 May 2013 05:51:21 GMT
Content-Length: 0
Connection: close
Set-Cookie: JSESSIONID=39AAB0E55F1AE44BC78DF27DB619C1F3; Path=/
Set-Cookie: JSESSIONID=39AAB0E55F1AE44BC78DF27DB619C1F3; Path=/
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
X-Origin: Memcached
```

Sunucu Bilgi ifşası

Server Error in '/' Application.

The resource cannot be found.

Description: HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable. Please review the following URL and make sure that it is spelled correctly.
Requested URL: /Manage/Kullanici/

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.2026

Server Error in '/' Application.

*The parameters dictionary contains a null entry for parameter 'lang' of non-nullable type
'
for method 'System.Web.Mvc.ActionResult
ChangeCulture(
'
, System.String)' in
''. An optional parameter must be a reference type, a nullable type, or
be declared as an optional parameter.
Parameter name: parameters*

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.ArgumentException:

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[ArgumentException: The parameters dictionary contains a null entry for parameter 'lang' of non-nullable type '
System.Web.Mvc.ActionDescriptor.ExtractParameterFromDictionary(ParameterInfo parameterInfo, IDictionary`2 parameters, MethodInfo methodInfo) +4
System.Linq.Enumerable.WhereSelectArrayIterator`2.MoveNext() +110
System.Linq.Enumerable.FirstOrDefault(IEnumerable`1 source) +46
System.Linq.Enumerable.Takirn(IEnumerable`1 source) +104
System.Web.Mvc.ReflectedActionDescriptor.Execute(ControllerContext controllerContext, IDictionary`2 parameters) +104
System.Web.Mvc.ControllerActionInvoker.InvokeActionMethod(ControllerContext controllerContext, ActionDescriptor actionDescriptor, IDictionary`2 parameters) +165
System.Web.Mvc.Async.<>c__DisplayClass39.<BeginInvokeActionMethodWithFilters>b__33() +125
System.Web.Mvc.Async.<>c__DisplayClass4f.<InvokeActionMethodFilterAsynchronously>b__49() +452
System.Web.Mvc.Async.<>c__DisplayClass37.<BeginInvokeActionMethodWithFilters>b__36(IAsyncResult asyncResult) +15
System.Web.Mvc.Async.<>c__DisplayClass2a.<BeginInvokeAction>b__20() +31
System.Web.Mvc.Async.<>c__DisplayClass25.<BeginInvokeAction>b__22(IAsyncResult asyncResult) +230
System.Web.Mvc.<>c__DisplayClass18.<BeginExecuteCore>b__18(IAsyncResult asyncResult) +28
System.Web.Mvc.<>c__DisplayClass17.<EndExecuteCore>b__3(IAsyncResult asyncResult ar) +20
System.Web.Mvc.Controller.EndExecuteCore(IAsyncResult asyncResult) +53
System.Web.Mvc.Async.<>c__DisplayClass4.<MakeVoidDelegate>b__3(IAsyncResult ar) +20
System.Web.Mvc.<>c__DisplayClass8.<BeginInProcessRequest>b__3(IAsyncResult asyncResult) +42
System.Web.Mvc.Async.<>c__DisplayClass4.<MakeVoidDelegate>b__3(IAsyncResult ar) +20
```

Server Error in '/' Application.

Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: Validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machineKey> configuration specifies the same validationKey and validation algorithm. AutoGenerate cannot be used in a cluster.

Source Error:

[No relevant source lines]

Source File: c:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files\root\4f526193\460a4778\App_Web_xj77zx0e.1.cs Line: 0

Stack Trace:

```
[ViewStateException: Invalid viewstate.
Client IP: 10.155.11.43
Port: 39069
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.31 (KHTML, like Gecko) chrome/26.0.1410.65 Safari/537.31
ViewState: /WEPOWUKLTqWnIE4NDk4Mw9KFgjCw9KAg8PZBYCHgdvbkNsawNrBrtyZXK1cm4gY2h1Y2tCZWVcmV1dwJtaxQoKTtkzejClh0zuozuyd3mAu5gB4q/wb1I
Referer: http://.../manage/Login.aspx
Path: /manage/Login.aspx]

[HttpException (0x80004005): validation of viewstate MAC failed. If this application is hosted by a Web Farm or cluster, ensure that <machinekey> config
System.web.UI.ViewStateException.ThrowError(Exception inner, String persistedState, String errorMessage, Boolean macValidationFailed) +148
System.web.UI.ViewStateException.PersistState(IStateFormatter formatter, String serializedState) +59
System.web.UI.HiddenField.PageStatePersister.Load() +10989784
System.web.UI.Page.LoadPageStateFromPersistenceMedium() +11074728
System.web.UI.Page.LoadAllState() +46
System.web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +11070247
System.web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +11069786
System.web.UI.Page.ProcessRequest() +91
System.web.UI.Page.ProcessRequest(HttpContext context) +240
ASP.manage.Login.aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files\root\4f526193\460a4778\App_Web_xj77zx0e.1.cs:47
System.web.CallHandlerExecutionStep.System.web.HttpApplication.IExecutionStep.Execute() +599
System.web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +171]
```

Version Information: Microsoft .NET Framework Version:2.0.50727.5466; ASP.NET Version:2.0.50727.5466

Not Found

The requested URL /jmx-console/ was not found on this server.

Oracle-Application-Server-10g/10.1.3.1.0 Oracle-HTTP-Server Server at portal Port 80

PHP Detaylı Bilgi İfşası

PHP Version 5.1.6

| | |
|-------------------------------------|--|
| System | Windows NT CICA30 5.2 build 3790 |
| Build Date | Aug 23 2006 16:31:18 |
| Configure Command | ccscript /nologo configure.js --enable-snapshot-build --with-gd=shared |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | enabled |
| Configuration File (php.ini) Path | C:\WINDOWS\php.ini |
| PHP API | 20041225 |
| PHP Extension | 20050922 |
| Zend Extension | 220051025 |
| Debug Build | no |
| Thread Safety | enabled |
| Zend Memory Manager | enabled |
| IPv6 Support | enabled |
| Registered PHP Streams | php, file, http, ftp, compress.zlib |
| Registered Stream Socket Transports | tcp, udp |
| Registered Stream Filters | convert.iconv*, string.rot13, string.toupper, string.toLowerCase, string.strip_tags, convert*, consumed, zlib* |

This program makes use of the Zend Scripting Language Engine:
Powered By
Zend Engine v2.1.0, Copyright (c) 1998-2006 Zend Technologies

PHP Credits

E-Posta Header Bilgi İfsaları

```
raffael:Desktop          curl --head
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 3463
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=5v5qusyifmwxppe13garurgn; path=/; HttpOnly
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 07 Nov 2013 21:41:43 GMT
```

İÇ PENETRASYON TESTİ SIZMA KANITLARI

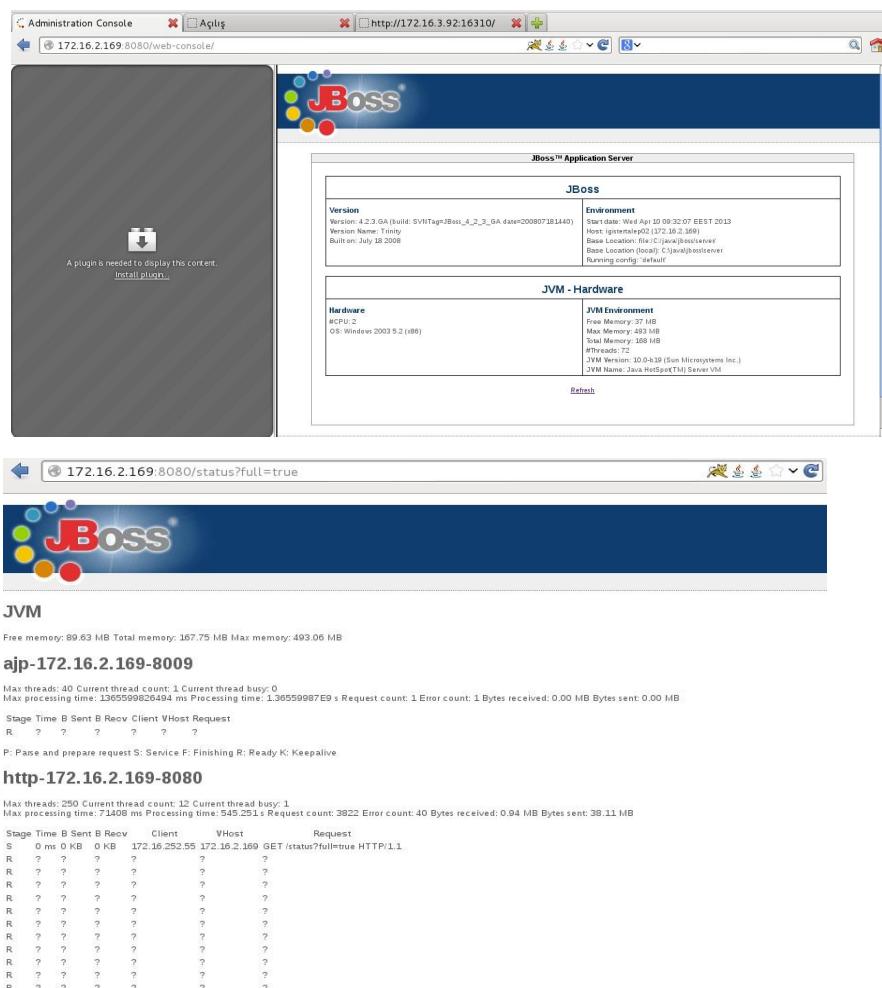
SNMP Metotları

```
msf auxiliary(snmp_login) > exploit
[*] :161SNMP - [001/118] - :           161 - SNMP - Trying public...
[+] SNMP: 10          community string: 'public' info: ''
[*] :161SNMP - [002/118] - 10.          161 - SNMP - Trying private...
[*] :161SNMP - [003/118] - 10.          161 - SNMP - Trying 0...
[*] :161SNMP - [004/118] - 10.          161 - SNMP - Trying 0392a0...
[*] :161SNMP - [005/118] - 10.          161 - SNMP - Trying 1234...
[*] :161SNMP - [006/118] - 10.          161 - SNMP - Trying 2read...
[*] :161SNMP - [007/118] - 10.          161 - SNMP - Trying 4changes...
[*] :161SNMP - [008/118] - 10.          161 - SNMP - Trying ANYCOM...
[*] :161SNMP - [009/118] - 10.          161 - SNMP - Trying Admin...
[*] :161SNMP - [010/118] - 10.          161 - SNMP - Trying C0de...
[*] :161SNMP - [011/118] - 10.          161 - SNMP - Trying CISCO...
[+] SNMP: 10.          'private' info: '' The quieter you become, t
[*] :161SNMP - [012/118] - 10.          161 - SNMP - Trying CR52401...
[*] :161SNMP - [013/118] - 10.          161 - SNMP - Trying IBM...
[*] :161SNMP - [014/118] - 10.          161 - SNMP - Trying ILM...
[*] :161SNMP - [015/118] - 10.          161 - SNMP - Trying Intermec...
[*] :161SNMP - [016/118] - 10.          161 - SNMP - Trying NoGaH$@!...
[*] :161SNMP - [017/118] - 10.          161 - SNMP - Trying OrigEquipMfr...
[*] :161SNMP - [018/118] - 10.          161 - SNMP - Trying PRIVATE...
[*] :161SNMP - [019/118] - 10.          161 - SNMP - Trying PUBLIC...
[*] :161SNMP - [020/118] - 10.          161 - SNMP - Trying Private...
```

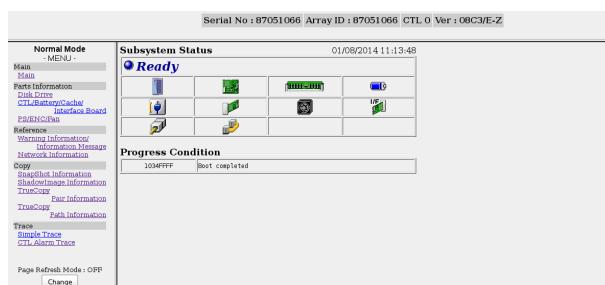
NFS Erişim

```
[+] NFS Export: /DataVolume/nguser [*]
[+] NFS Export: /DataVolume/Public [*]
[+] NFS Export: /DataVolume/Download [*]
[+] NFS Export: /DataVolume/teknisyen [*]
[+] NFS Export: /DataVolume/natek_backup [*]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Jboss Uygulama Platformu Çoklu Zafiyetler Serisi



Servis Bilgi İfşası





0 850 333 50 03

Esentepe Mah. Kore Şehitleri Cad. No:42 Zincirlikuyu - Şişli / İSTANBUL
Tel: 0850 333 50 03 Fax: 0212 278 35 38 info@uitsec.com www.uitsec.com