Siber Güvenlik Red Team Raporu 2025

HAZIRLAYANLAR

UYGAR YASİN AYDIN
ALPEREN SABUNCUOĞLU

İletişim

0216 232 24 33 - 0312 911 4640

www.nesilteknoloji.com

2025 RAPORU

PENTESTTE Kritik 10 bulgu

MERHABA DÜNYA.

Güvenlik reaktif değil, proaktif olmalıdır.

Teknoloji hızla gelişirken, kurumların işlediği kişisel verilerin hacmi ve çeşitliliği de büyüyor. Dijital öncelikli dünyada siber riskler artık “olursa bakarız” denecek bir konu değil; sürekliliği olan ve etkisi artan bir gerçek. KVKK kapsamında yaşanabilecek bir ihlal; yalnızca teknik bir problem değil, aynı zamanda idari yaptırımlar, itibar kaybı, iş sürekliliği etkisi ve müşteri güveninin zedelenmesi anlamına gelir.

Bu sadece bir uyarı değil. Veri koruma kültürü için net bir dönüşüm çağrısıdır.
Bugünün BT ve güvenlik liderleri, yalnızca dokümantasyon ve kontrol listeleriyle yetinemez. KVKK uyumu ve sözleşmesel yükümlülükler, teknik kontrollerin gerçek dünyada çalıştığının kanıtlanmasını gerektirir. Ancak geleneksel yaklaşımlarda penetrasyon testleri çoğu zaman yılda bir kez yapılır; bu da yeni zafiyetlerin ve yanlış yapılandırmaların uzun süre fark edilmemesine neden olur. Özellikle kişisel veri işleyen sistemlerde (web uygulamaları, API’ler, mobil uygulamalar, AD/LDAP, e-posta, dosya sunucuları, bulut depoları) bu risk kabul edilebilir değildir.

Nesil Teknoloji olarak daha etkili bir yaklaşım sunuyoruz.
KVKK ve veri koruma odağında yürüttüğümüz penetrasyon testleri; kurumunuzun kişisel veri işleme süreçlerini hedef alan gerçekçi saldırı senaryolarıyla riskleri görünür kılar. Çalışmalarımız;

- Kişisel veri envanteriyle uyumlu kapsamlandırma,
- Yetkisiz erişim ve ayrıcalık yükseltme senaryoları,
- Web/API güvenliği (OWASP) ve kimlik doğrulama zafiyetleri,
- Ağ içi hareket (lateral movement) ve AD güvenliği,
- Veri sızıntısı (exfiltration) ve log/izleme zafiyetleri,
- Şifreleme, erişim kontrolü, yedekleme ve saklama politikaları
- gibi başlıklarda sonuç odaklı bulgular üretir.

Bu modern yaklaşım sayesinde kurumlar; daha sık, ölçeklenebilir ve maliyet-etkin testlerle yıl boyunca güvenlik duruşunu izleyebilir. Çünkü veri koruma tarafında “yılda bir kez test” yaklaşımı artık yeterli değildir. 2025 yaklaşımıyla Nesil Teknoloji, KVKK kapsamındaki sistemler için gerçekleştirilen testlerde en sık karşılaşılan kritik veri koruma risklerini ve bunlara karşı öncelikli aksiyonları raporlar. Bu çalışma; güvenlik ekiplerinin güncel kalmasına, denetim süreçlerine hazır olmasına ve riskleri proaktif şekilde azaltmasına yardımcı olur. Nesil Teknoloji KVKK Danışmanlığı • Veri Koruma • Penetrasyon Testi • Siber Güvenlik

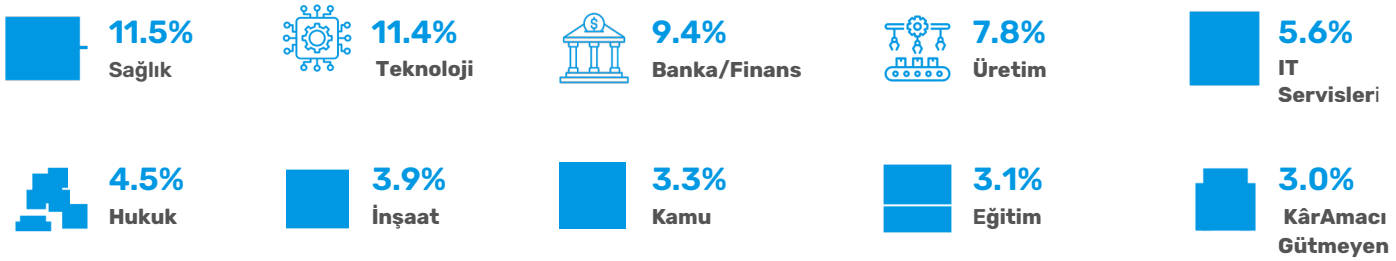
İÇİNDEKİLER

NESİL TEKNOLOJİ

NesilTeknoloji uzunyıllardır tam kapsamlı penatrasyon testi ile 20.000'den fazla kuruluşa hizmet vermiştir. Bu rapor, 2025 yılında hizmet vermiş olduğumuz işletmeler aracılığıyla dünya genelinde gerçekleştirilen 9.000'den fazla güvenlik testi sonuçlarına dayanarak en kritik 10 ağ pentest bulgusunu göstermektedir.

GÖRÜLME YÜZDESİNE GÖRE EN KRİTİK 10 İÇ AĞ (INTERNAL) PENTEST BULGUSU.

- **66.0 %** Multicast DNS (mDNS) Sahteciliği
- **61.6 %** NetBIOS Name Service Sahteciliği
- **57.0 %** Link-Local Multicast Name Sahtecilliği
- **47.2 %** IPv6 DNS Sahteciliği
- **21.8 %** Güncel Olmayan (Eski) Microsoft Windows Sistemleri
- **12.6 %** IPMI Kimlik Doğrulama Atlama
- **4.1 %** Microsoft Windows Uzak Kod Çalıştırma (RCE) – EternalBlue
- **3.8 %** Microsoft Windows Uzak Kod Çalıştırma (RCE) – BlueKeep
- **1.4 %** Firebird Sunucularının Varsayılan Kimlik Bilgilerini Kabul Etmesi
- **1.2 %** Active Directory Certificate Services (AD CS) Yetki Yükseltme Zafiyetleri



TANIMLAR

PENTEST BULGULARI

Bulgular,kurumungüvenlik duruşunu etkileyen kritik zafiyet ve konfigürasyon eksikliklerini ifade eder. Nesil Teknoloji tarafından doğrulanmış olup rapor boyunca “Bulgular” olarak geçer.

PENTEST BULGULARI

Sızma Testiekibimizin iç ve dış ağlarda kesintiye neden olmayacak şekilde gerçekleştirdiği değerlendirme sırasında başarıyla sömürülen (exploited) güvenlik açıklarıdır. Raporda “PenTest bulguları” ifadesi boyunca kısaca “Bulgular” olarak anılacaktır.
Kuruluşların bulguları önceliklendirmesine yardımcı olmak için, pentest bulguları ve gözlemler CVSS (Common Vulnerability Scoring System) tabanlı tehdit seviyesi derecelendirmeleriyle kategorize edilir. CVSS, bir zafiyetin temel özelliklerini standart şekilde tanımlayarak ciddiyetini yansıtan sayısal bir skor üretir. CVSS’nin güncel sürümü 3.1’dir.

Severity	Description
Kritik CVSS 9.0-10.0	Kritik seviye, acil düzeltme veya azaltma gerektirir. Bu zafiyetlerin sömürülmesi saldırgan açısından genellikle düşük efor gerektirir; ancak kuruluşun sistemleri ve verilerinin gizliliği, bütünlüğü ve/veya erişilebilirliği için ciddi tehdit oluşturur. Bu seviyedeki bir bulgunun başarılı şekilde istismar edilmesi, birden fazla sisteme ve/veya birden çok hassas bilgiye erişimle sonuçlanabilir.
Yüksek CVSS 7.0-8.9	Yüksek seviye, acil düzeltme veya azaltma gerektirir. Bu zafiyetlerin sömürülmesi saldırgan açısından genellikle düşük efor gerektirir ve kuruluşun sistemleri/verileri için önemli bir risk doğurur. Bu seviyedeki bir bulgunun istismarı, tek bir erişim noktasına veya sınırlı hassas bilgiye erişime yol açabilir
Orta CVSS 4.0-6.9	Orta seviye, kısa ve makul bir süre içinde düzeltme veya azaltma gerektirir. Bu bulgular; sistemler/uygulamalar üzerinde yetkisiz (ayrıcalıksız) kullanıcı hesaplarının ele geçirilmesine yol açabilir veya ana makine/hizmet/uygulama için Hizmet Dışı Bırakma (DoS) durumuna işaret edebilir.
Düşük CVSS 0.1-3.9	Düşük seviye, daha yüksek öncelikli bulgular giderildikten sonra düzeltme veya azaltma gerektirir. Bu bulgular genellikle yetkisiz veya anonim kullanıcılara bilgi sızdırır ve diğer saldırı vektörleriyle birleştirildiğinde daha ciddi saldırılara zemin hazırlayabilir.
Bilgi CVSS 0	Bilgilendirici seviye, ortam için önemli bir tehdit oluşturmaz. Değerli bilgi ifşasına neden olabilecek bulgular olabilir ancak kuruluşa yönelik doğrudan teknik bir saldırıyı mümkün kılmaz. Bu seviyedeki bulgular, saldırganın kurum hakkında bilgi toplamasına yardımcı olabilir ve örneğin sosyal mühendislik veya oltalama (phishing) gibi saldırılarda kullanılabilir.

Görülme Sıklığı:66%

01 MULTICAST DNS (mDNS) SAHTECİLİĞİ

MulticastDNS(mDNS),yerel ağlar için bir isimçözümleme (name resolution) protokolüdür ve özel bir DNS sunucusunun erişilemediği durumlarda alanadlarının çözülmesini kolaylaştırır. Çözümleme süreci şu aşamalarda gerçekleşir:

1. Sistemönce uygunDNSadı/IPadreseşleştirmeleriiçin yerelhosts dosyasınabakar.

2. Yapılandırılmış bir DNS sunucusu yoksa sistem mDNS'ye başvurur ve DNS adına karşılık gelen host'tan kimlik bilgisi istemek için IP multicast sorgusu yayınlar. Bu protokol davranışı, kötü niyetli aktörlerin bu sorgulara yanıt vererek meşru sistemleri taklit etmesine (impersonation) imkân tanıyan potansiyel bir zafiyet oluşturu

ÖNERİLER

- mDNS spoofing riskini azaltmak için birincil öneri, kullanım gerekmiyorsa mDNS'nin tamamen devre dışı bırakılmasıdır. Windows sistemlerde bu genellikle "Disable Multicast Name Resolution" grup ilkesi ile yapılabilir. Birçok uygulama mDNS işlevini yeniden devreye alabileceğinden alternatif olarak Windows Firewall üzerinden UDP 5353 portunu engellemek de bir seçenektir. Windows dışı sistemlerde Apple Bonjour veya avahi-daemon gibi servisleri devre dışı bırakmak benzer koruma sağlayabilir.

- mDNS'nin devre dışı bırakılmasının ekran yansıtma (screen casting) ve bazı toplantı odası teknolojileri gibi işlevleri bozabileceği unutulmamalıdır. Tamamen kapatmak mümkün değilse, etkilenen sistemleri kontrollü bir ağ segmentinde izole etmeyi ve bu sistemlere erişen hesaplarda güçlü/karmaşık parolaları zorunlu kılmayı değerlendirin.

TEKRARLAMA ADIMLARI

mDNS yapılandırılmış bir sistemde, geçersiz olduğu bilinen bir DNS adıyla (örn. test123.local) etkileşim kurmayı deneyin. Başka bir sistemde ise Wireshark gibi bir ağ paket analizörü kullanarak, iç ağ ortamındaki mDNS trafiğini UDP 5353 portu üzerindeki UDP sorgularına göre filtreleyip inceleyin.

GÜVENLİK ETKİSİ

CVSS3.1
9.8

Yerelsubnet üzerinden iletilen mDNSsorguları, bunları alabilen herhangibir cihaz tarafından yanıtlanabilir. Bu zafiyet, saldırganın kendi sisteminin IP adresiyle yanıt vererek sorgu yapan sistemi yanıltmasına olanak tanır. Bu tür bir istismar; kurbanın erişmeye çalıştığı servise bağlı olarak (ör. SMB, HTTP, MSSQL) şunlara yol açabilir:

- Şifrelenmemiş ya da hash'lenmiş kimlik bilgileri dâhil hassas bilgilerin ele geçirilmesi / araya girme (interception) Hash'lenmiş
- kimlik bilgilerinin modern hesaplama gücü ve brute-force yöntemleriyle nispeten kısa sürede kırılabilmesi nedeniyle hesap ele geçirme riski

REFERANSLAR

- **Multicast DNS**

Görülme Sıklığı:66%

02 NETBIOS NAME SERVICE (NBNS) SAHTECİLİĞİ

NetBIOS NameService (NBNS), bir DNS sunucusu kullanılamadığında veyayanıt vermediğinde, iç ağdaki iş istasyonlarının alan adlarını çözümlemekiçinkullandığı bir protokoldür. Bir sistem bir DNS adını çözmeye çalıştığında şu adımları izler:

1. Sistem, DNS adını bir IP adresine eşleyen bir kayıt olup olmadığını görmek için önce yerel hosts dosyasını kontrol eder.
2. Yerel bir eşleme yoksa, ilgili IP adresini almak için yapılandırılmış DNS sunucu(lar)ına bir DNS sorgusu gönderir.
3. DNS sunucu(ları) adı çözemiyorsa, sistem yerel ağ genelinde bir NBNS yayını (broadcast) yapar ve diğer sistemlerden yanıt ister.

DNS sunucu(ları) adı çözemiyorsa, sistem yerel ağ genelinde bir NBNS yayını (broadcast) yapar ve diğer sistemlerden yanıt ister.

ÖNERİLER

- NBNS spoofing riskini azaltmak için, iç ağdaki tüm istemcilerde NetBIOS servisinin devre dışı bırakılması önerilir. Bu işlem;
  - DHCP seçeneklerinin yapılandırılması,
  - ağ bağdaştırıcısı (network adapter) ayarlarının düzenlenmesi, veya Windows Registry üzerinde değişiklik
  - yapılması gibi farklı yöntemlerle gerçekleştirilebilir. Bu
  - değişikliklerin uygulanması, NBNS ile ilişkili potansiyel saldırı yüzeyini önemli ölçüde azaltır.

TEKRARLAMA ADIMLARI

NBNS yapılandırılmış bir sistemde, geçersiz olduğu bilinen bir DNS adıyla (örn. test123.local) etkileşim kurmayı deneyin. Başka bir sistemde ise Wireshark gibi bir ağ paket analizörü kullanarak iç ağ ortamındaki broadcast trafiğini inceleyin.

GÜVENLİK ÖNERİLERİ

CVSS3.1
9.8

NBNSsorgularının yayın (broadcast) yapısı, yerel ağdaki herhangi bir sistemin yanıt verebilmesi anlamına gelir. Bu zafiyet; saldırganın bu sorguları kendi IP adresiyle yanıtlayarak trafiği meşru servislerden saldırgan sistemine yönlendirmesi ile istismar edilebilir. Örneğin SMB, MSSQL veya HTTP gibi servisler, farkında olmadan saldırgan sisteme şu verileri gönderebilir:

- Hassas veriler
- Düz metin (plaintext) veya hash'lenmiş hesap kimlik bilgileri

Ayrıca modern hesaplama imkanları, hash'lenmiş kimlik bilgilerinin kırılmasını kolaylaştırabilir ve bu da kullanıcı hesaplarına yetkisiz erişim riskini artırabilir.

REFERANSLAR

- **MITRE ATT&CK – LLMNR/NBT-NS Zehirleme (Poisoning) ve SMB Aktarma (Relay) (T1557.001)**

Görülme Sıklığı:57%

03 LINK-LOCAL MULTICAST NAME RESOLUTION (LLMNR) SAHTECİLİĞİ

Link-LocalMulticast NameResolution (LLMNR),içağ ortamındakiiş istasyonlarıarasında; bir DNS sunucusu olmadığında veya yardımcı olamadığında bir alan adı/sistem (DNS) adını çözümlemek için kullanılan bir protokoldür. Bir sistem bir DNS adını çözmeye çalıştığında şu adımları izler:

1. Sistem, ilgili DNS adını bir IP adresiyle eşleştiren bir kayıt olup olmadığını belirlemek için yerel hosts dosyasını kontrol eder
2. Yerel hosts dosyasında kayıt yoksa, sistem ilgili DNS adına karşılık gelen IP adresini almaya çalışmak için yapılandırılmış DNS sunucu(lar)ına bir DNS sorgusu gönderir.
3. Yapılandırılmış DNS sunucu(lar)ı DNS adını IP adresine çözemiyorsa, sistem yerel ağda diğer sistemlerden yardım almak için bir LLMNR broadcast paketi gönderir.

GÜVENLİK ETKİSİ

CVSS3.1
9.8

LLMNRsorgularıağ genelinde broadcast edildiği için, ağdaki herhangi bir sistem bu sorgulara yanıt verebilir. Bu durum kötü niyetli aktörler tarafından suistimal edilebilir; saldırgan, ilgili sorguların tamamına kendi sisteminin IP adresiyle yanıt vererek kurbanı yanıltabilir. Kurbanın erişmeye çalıştığı servise bağlı olarak (ör. SMB, MSSQL, HTTP vb.), saldırgan düz metin (cleartext) ve/veya hash'lenmiş hesap kimlik bilgilerini ele geçirebilir. Hash'lenmiş kimlik bilgileri, günümüz hesaplama gücü ve brute-force teknikleriyle çoğu zaman nispeten kısa sürede geri elde edilebilir/kırılabilir.

ÖNERİLER

LLMNR spoofing ile ilişkili riskleri azaltmak için, etkilenen sistemlerde LLMNR işlevinin devre dışı bırakılması kritik önem taşır. Bu aşağıdaki yöntemlerle yapılabilir:

- **Grup İlkesi (Group Policy) ile Yapılandırma:** Computer Configuration\Administrative Templates\Network\DNS Client yoluna gidin ve "Turn off Multicast Name Resolution" ayarını Enabled yapın. (Windows Server 2003 domain controller üzerinde yapılandırma yönetimi için Windows 7'de bulunan RSAT (Remote Server Administration Tools) kullanılabilir; ilgili bağlantıya yönlendirme yer alır.)
- **Windows Vista/7/10 Home sürümleri için Registry Değişikliği: Registry'de şu yolu açın: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient ve EnableMulticast anahtarını 0 yapın veya özelliği kapatmak için kaldırın.**

REFERENCES

- **Aradaki Saldırgan (Adversary-in-the-Middle): LLMNR/NBT-NS Zehirleme (Poisoning) ve SMB Aktarma (Relay)**
- **Windows için Uzak Sunucu Yönetim Araçları (RSAT)**

TEKRAR ADIMLARI

LLMNR yapılandırılmış bir sistemde, geçersiz olduğu bilinen bir DNS adıyla (örn. test123.local) etkileşim kurmayı deneyin. Başka bir sistemde ise Wireshark gibi bir ağ paket analizörü kullanarak iç ağ ortamındaki broadcast trafiğini inceleyin.

Görülme Sıklığı:47.2%

04 IPV6 DNS SAHTECİLİĞİ

IPv6DNSspoofing riski, iç ağ altyapısına kötü niyetli (rogue) bir DHCPv6 sunucusunun dahil edilmesiyle ortaya çıkabilir. Microsoft Windows sistemlerinin IPv6'yı IPv4'e tercih etmesi nedeniyle, IPv6 destekli istemciler IP adresi yapılandırmalarını mevcut herhangi bir DHCPv6 sunucusundan almaya daha yatkındır.

ÖNERİLER

- **Ağ Katmanında Rogue DHCP'yi Yönetme:**
  Yetkisiz DHCP sunucularını kontrol altına almak ve DNS spoofing saldırı ihtimalini azaltmak için switch ve firewall üzerinde Rogue DHCP tespiti, DHCP snooping ve DHCP kimlik doğrulaması gibi özellikleri uygulayın.

- **IPv6 yerine IPv4'ü Tercih Ettirme:**
  Grup İlkesi Nesneleri (GPO) veya Grup İlkesi Tercihleri (GPP) ile registry değişiklikleri dağıtarak Windows sistemlerini IPv6 yerine IPv4'ü tercih edecek şekilde yapılandırın. Bu yaklaşımın Windows dışı cihazlarda saldırıyı engellemeyebileceğini unutmayın.

- **IPv6'yı Devre Dışı Bırakma: Microsoft Windows sistemlerde genellikle tavsiye edilmese de, iş süreçlerinde ciddi kesinti yaratmadığı testlerle doğrulanırsa son çare önlem olarak IPv6'nın devre dışı bırakılması değerlendirilebilir.**

TEKRARLAMA ADIMLARI

Kali Linux içindeki "mitm6" aracı kullanılarak, yerel ağda hızlıca bir DHCPv6 sunucusu devreye alınabilir ve IPv6 etkin istemcilere (varsayılan olarak) 5 dakikalık kira süreleri (lease) atanabilir.

GÜVENLİK ETKİSİ

CVSS3.1
10.0

Kötü niyetli bir DHCPv6 sunucusunun devreye alınması, IPv6 etkin istemcileri saldırganın sistemini DNS sunucusu olarak kullanmaya yönlendirerek saldırganın DNS isteklerini manipüle etmesine imkan tanır. Bu yetenek; kullanıcı kimlik bilgileri dahil hassas verilerin yetkisiz şekilde ele geçirilmesi gibi ciddi sonuçlara yol açabilir. Tüm DNS sorguları saldırganın sunucusuna çözümlendiğinde, kurban sistem farkında olmadan saldırganın altyapısında çalışan kötü amaçlı servislerle iletişim kurabilir. Bu durum SMB, HTTP, RDP ve MSSQL gibi platformları kapsayabilir.

REFERANSLAR

- **IPv6 Ağlarını Ele Geçirme (Taking Over IPv6 Networks)**
- **İleri Seviye Kullanıcılar İçin: Windows'ta IPv6 Yapılandırma Rehberi (configuring IPv6 in Windows for advanced users)**

Görülme Sıklığı:21.8%

05 GÜNCEL OLMAYAN MICROSOFT WINDOWS SİSTEMLERİ (OUTDATED MICROSOFT WINDOWS SYSTEMS)

GüncelolmayanMicrosoft Windows sistemleri, Microsoft'tanartıkkritik güncellemeler almadıkları için önemli güvenlik riskleri oluşturur. Bu sistemlerde, bilinen zafiyetleri gideren kritik güvenlik yamaları eksik olabilir; bu da onları saldırganların istismarına daha açık hale getirir. Ayrıca güncelleme eksikliği, modern güvenlik araçları ve yazılımlarıyla uyumluluk sorunlarına yol açabilir ve sistemin savunmasını daha da zayıflatabilir. Güncel olmayan sistemlerdeki zafiyetler; kötü amaçlı yazılım yayma, veri sızdırma (data exfiltration) ve yetkisiz erişim gibi saldırılarda sıkça istismar edilebilir.

GÜVENLİK ETKİSİ

CVSS3.1

9.8

Güncel olmayan bir Microsoft Windows sistemi istismar edilirse, saldırgan etkilenen sisteme/sistemlere yetkisiz erişim elde edebilir ve hassas verileri ile kaynakları açığa çıkarabilir. Ayrıca aynı ağdaki sistemler arasında yapılandırma benzerliği bulunması nedeniyle saldırgan, ele geçirilen sistemi bir sıçrama noktası olarak kullanarak yatay hareket (lateral movement) gerçekleştirebilir; ek sistemleri de ele geçirip ihlalin genel etkisini/boyutunu büyütebilir.

ÖNERİLER

Üretici tarafından hâlâ desteklenen güncel işletim sistemlerine geçilerek, güncel olmayan Microsoft Windows sürümlerinin değiştirilmesi önemle tavsiye edilir. Bu kapsamda, güncel olmayan sürümleri tespit etmek ve önceliklendirmek için tüm sistemlerde ayrıntılı bir envanter çalışması yapılmalı; ardından kademeli (phased) bir yükseltme stratejisi uygulanmalıdır. Güvenlik bütünlüğünü korumak için tüm sistemlerin en son güncellemeleri ve yamaları düzenli olarak aldığı doğrulanmalıdır.

TEKRARLAMA ADIMLARI

Etkilenen hedeflerin spesifik sürümlerini tespit etmek için Nmap veya Metasploit gibi bir işletim sistemi tanımlama tarayıcısı kullanarak tarama yapın. Alternatif olarak bir ağ yöneticisi sisteme giriş yapıp sistem özellikleri üzerinden işletim sistemi sürümünü kontrol edebilir.

REFERENCES

- **MITRE ATT&CK Mitigations – Update Software**
- **Windows desteklenmiyorsa (supported değilse) ne anlama gelir?**

Görülme Sıklığı:12.6%

06 IPMI KİMLİK DOĞRULAMA ATLAMA

IntelligentPlatformManagement Interface (IPMI), ağ yöneticilerinin sunucularımerkeziolarak yönetmesi için kullanılan kritik bir donanım/yönetimarayüzüdür. IPMI ile donatılmış sunucu(lar)ın yapılandırılması sırasında, saldırganların uzaktan kimlik doğrulama mekanizmasını atlamasına izin verebilecek bazı zafiyetler bulunabilir. Bu durum parola hash'lerinin ele geçirilmesine yol açar; varsayılan veya zayıf hashleme algoritmalarının kullanıldığı durumlarda saldırganlar parolaları düz metin (cleartext) olarak da geri elde edebilir.

ÖNERİLER

Bu zafiyet için bir yama bulunmadığı göz önüne alındığında, aşağıdaki azaltım (mitigation) stratejilerinden bir veya birkaçının uygulanması kritik önem taşır:

- IPMI erişimini yalnızca yönetim fonksiyonuna ihtiyaç duyan yetkili sistemlerle sınırlandırın.
- İş süreçleri için gerekmeyen sunucu(lar)da IPMI servisini devre dışı bırakın.
- Varsayılan yönetici parolalarını güçlü ve karmaşık parolalarla değiştirin.
- Hassas kimlik bilgilerinin açığa çıkmasına neden olabilecek ortadaki adam (MITM) saldırı riskini azaltmak için HTTPS ve SSH gibi güvenli iletişim protokollerini kullanın.

GÜVENLİK ETKİSİ

CVSS3.1
10.0

Düz metinparolaların elde edilebilmesi, ciddi bir güvenlik riski oluşturur; çünkü saldırgan bu bilgileri kullanarak SSH, Telnet veya web tabanlı yönetim arayüzleri dahil olmak üzere hassas servislere yetkisiz uzaktan erişim elde edebilir. Bu tür bir yetkisiz erişim; yapılandırmaların değiştirilmesine, servislerin erişilebilirliğinin ve bütünlüğünün olumsuz etkilenmesine yol açabilir (ele geçirilen sunucu(lar) üzerindeki servisler dâhil).

TEKRARLAMA ADIMLARI

Metasploit framework kullanılarak, etkilenen servise karşı aşağıdaki modül yapılandırılıp çalıştırılır:

```
auxiliary/scanner/ipmi/ipmi_dumphashes
```

REFERENCES

- **IPMI Nedir ve Neden Önemlidir? – Cipher Suite Zero ile Kimlik Doğrulama Atlama**
- **IPMI "Cipher Suite Zero" Kimlik Doğrulama Atlama Zafiyeti**
- **IPMI "Cipher Suite Zero" Zafiyetlerini Tespit Etme ve Düzeltme (Birden Fazla Üretici)**

Görülme Sıklığı:4.1%

07 WINDOWS UZAKTAN KOD ÇALIŞTIRMA (RCE) – ETERNALBLUE

EternalBlue, Microsoft ServerMessageBlock (SMBv1)protokolünde bulunanbir uzaktan kod çalıştırma (Remote Code Execution) zafiyetidir. Saldırganın, zafiyetli bir sisteme özel olarak hazırlanmış paketler göndermesine imkân tanır ve bu sayede yetkisiz erişim ile sistem seviyesinde ayrıcalıklarla keyfi kod çalıştırılmasına yol açabilir.

ÖNERİLER

EternalBlue zafiyetiyle ilişkili riski azaltmak için, etkilenen tüm sistemlere ilgili güvenlik yamalarının gecikmeden uygulanması zorunludur. Ayrıca kurumun yama yönetimi süreci ayrıntılı şekilde gözden geçirilerek bu sistemlerin yamalanmamış durumda kalmasına neden olan eksiklikler tespit edilmelidir. Bu zafiyetin yüksek riski ve yaygın istismar edilmesi nedeniyle acil iyileştirme çalışmaları kritiktir.

TEKRARLAMA ADIMLARI

Yalnızca yetkili ve kontrollü bir ortamda, güvenilir bir zafiyet tarayıcısı veya onaylı sızma testi araçlarıyla SMBv1/MS17-010 kapsamında zafiyet doğrulaması yapılarak kontrol edilebilir.

GÜVENLİK ETKİLERİ

CVSS3.1
9.8

EternalBlue istismar edildiğinde saldırgan, etkilenen sistem üzerinde tam kontrol elde edebilir. Bu genellikle kurum içinde ek saldırılara yol açar; düz metin parolalar ve hash'lerin çıkarılması ile ağ içinde yatay hareket (lateral movement) gibi etkiler görülebilir. Bu zafiyetin istismarı, hedef sistem üzerinde ayrıca bir ayrıcalık yükseltme gerektirmediğinden, saldırgan çoğu durumda ele geçirilen sistem üzerinde keşif/enum işlemlerine başlamak için ihtiyaç duyduğu erişimi elde etmiş olur.

REFERANSLAR

- **Microsoft Windows SMB Server için Güvenlik Güncellemesi (4013389)**

Görülme Sıklığı:3.8%

08 WINDOWS UZAKTAN KOD ÇALIŞTIRMA (RCE) – BLUEKEEP

Testlersırasında,Microsoft Windowssistemlerindebulunan CVE-2019-0708(BlueKeep)zafiyetine açık sistemler tespit edilmiştir. Bu zafiyet; zayıflıktanfaydalanabilen araç ve kodların erişilebilir olması nedeniyle saldırganlaraçısından son derece değerlidir. Bu zafiyetin başarılı şekilde istismar edilmesi,genellikle istismar edilen sisteme/sistemlere tam erişim ile sonuçlanır.

ÖNERİLER

BlueKeep zafiyetine ilişkin riski azaltmak için, etkilenen sistemlere ilgili güvenlik güncellemelerinin ivedilikle uygulanması kritik önem taşır. Kuruluşlar, zamanında güncelleme yapılamamasına katkıda bulunan faktörleri tespit etmek için yama yönetimi süreçlerini kapsamlı şekilde gözden geçirmelidir. Bu zafiyetin istismar edilebilirliği ve sistemleri ciddi şekilde tehlikeye atabilmesi nedeniyle, kurumun dijital ortamını korumak için acil aksiyon gereklidir.

TEKRARLAMA ADIMLARI

```
exploit/windows/rdp/cve_2019_0708_bluekeep_rce
```

Yalnızca yetkili ve kontrollü bir ortamda, onaylı güvenlik test araçlarıyla CVE-2019-0708 kapsamında zafiyet doğrulaması yapılabilir. Not: Bu tür testler bazı durumlarda hedef sistemin erişilebilirliğini etkileyebileceğinden dikkatle planlanmalıdır

GÜVENLİK ETKİSİ

CVSS3.1
9.8

BlueKeep zafiyetinin istismar edilmesiyle saldırgan, etkilenen sistem üzerinde tam kontrol elde edebilir. Bu durum çoğu zaman kurum içinde ek saldırılara yol açar; düz metin parolalar ve hash'lerin çıkarılması ile ağ içinde yatay hareket (lateral movement) gibi etkiler görülebilir. Bu zafiyetin istismarı hedef sistem üzerinde ayrıca bir ayrıcalık yükseltme gerektirmediğinden, saldırgan genellikle ele geçirilen sistemde keşif/enum süreçlerine başlamak için ihtiyaç duyduğu erişimi elde etmiş olur.

REFERENCES

- **Uzak Masaüstü Hizmetleri (RDP) Uzaktan Kod Çalıştırma Zafiyeti (Remote Code Execution Vulnerability)**

Görülme Sıklığı:1.4%

09 FIREBIRD SUNUCULARI VARSAYILAN (DEFAULT) KİMLİK BİLGİLERİNİ KABUL EDİYOR

Varsayılankimlik bilgileri, genellikle ilk kurulumiçindüşünülmüşve çoğuzamansistemiçine “gömülü” kullanıcı adı/parolalardır; güvenliği korumakiçinhızla değiştirilmelidir. Bu sorun, sistemler yeniden yapılandırılmadan devreye alındığında veya kurulum sırasında varsayılan ayarlar gözden kaçırıldığında ortaya çıkar.

ÖNERİLER

Bu zafiyeti azaltmak için Firebird sunucularıyla ilişkili varsayılan kimlik bilgilerinin GSEC aracı kullanılarak değiştirilmesi kritik önem taşır. Ek olarak;

- Düzenli kimlik bilgisi denetimleri (credential audit) için bir politika oluşturun.
- Canlıya almadan önce tüm varsayılan ayarların değiştirildiğini doğrulayın.
- Yetkisiz denemeleri yakalamak için sunucu erişim loglarını sürekli izleyin ve şüpheli aktiviteler için alarm/uyarı mekanizmalarını etkinleştirin.

Bu yaklaşım, olası istismar girişimlerini erken tespit etmeye yardımcı olur.

TEKRAR ADIMLARI

Yalnızca yetkili ve kontrollü bir ortamda; Firebird servisinin varsayılan kimlik bilgilerini kabul edip etmediğini doğrulamak için, güvenli test yöntemleriyle doğrulama yapılabilir. Test sırasında sistemde beklenmedik değişiklik oluşmaması için süreç dikkatle planlanmalı ve kayıt altına alınmalıdır.

```
# isql-fb SQL> CREATE DATABASE
'<host_ip>/3050:C:\firebird_default_creds_test.txt' user
'SYSDBA' password 'masterkey';
```

```
I/O error during "CreateFile (create)" operation for file "
<database_filename>"
-Error while trying to create file
-Access is denied.
```

To remove the created database, run the following command in isql-fb:

```
SQL> drop database;
```

SECURITY IMPACT

CVSS3.1
9.0

Firebird sunucularında varsayılan kimlik bilgilerine güvenilmesi, yetkisiz erişime yol açabilir ve saldırganların etkilenen sistemlerde kimlik doğrulayıp keşif (reconnaissance) yapmasına imkan tanır. Saldırganlar dosyaları listeleyebilir veya sistem yapılandırmalarını değiştirerek daha ileri istismar için yeni yollar açabilir. Eğer saldırgan Firebird veritabanı dosyalarının konumunu tespit ederse, hassas veritabanı verilerini okuma veya değiştirme yeteneği kazanabilir. Ayrıca Firebird’ün bazı sürümleri sistem komutlarını çalıştıracak şekilde suistimal edilebilir; bu da saldırganın uzak sistem üzerindeki kontrolünü genişletebilir.

REFERENCES

- **Sunucu yapılandırması ve yönetimi (Server configuration and management)**

Görülme Sıklığı:1.2%

10 ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS) YETKİ YÜKSELTME ZAFİYETLERİ

Active Directory Certificate Services (AD CS) Yetki Yükseltme (Elevation of Privilege) zafiyetleri; Microsoft AD CS içinde tespit edilen çeşitli güvenlik zayıflıklarını kapsar. Bu zafiyetler çoğunlukla, belirli AD CS Registry anahtarlarına atanmış güvensiz varsayılan izinlerden kaynaklanır. Belirli koşullar altında bir saldırgan, bu zafiyetleri istismar ederek Active Directory ekosistemi içinde yetkisiz şekilde daha yüksek ayrıcalıklar elde edebilir.

GÜVENLİK ETKİSİ

CVSS3.1
10.0

Tespitedilen zafiyetlerden bir veya birkaçının istismar edilmesi, saldırganın daha düşük seviyeli hesaplardan yetki yükselterek Active Directory yapısı içinde daha üst seviye erişim elde etmesine imkan tanıyabilir. Bu erişim; ağ içinde bulunan hassas, kuruma özel veya sınıflandırılmış verilerin ele geçirilmesini kolaylaştırabilir.
Ayrıca sertifika servislerinin ele geçirilmesi, tüm altyapı genelinde bütünlük (integrity) ve güvenlik ihlallerine yol açabilecek ciddi sonuçlar doğurabilir; tehdit aktörlerinin servisleri temelden manipüle etmesine veya kötüye kullanmasına imkan tanıyabilir.

ÖNERİLER

AD CS ile ilişkili bu tür zafiyetleri gidermek için kurumların, Microsoft tarafından yayınlanan ilgili güvenlik yamaları ve güncellemeleri ivedilikle uygulaması kritik önem taşır. Ayrıca AD CS Registry anahtarlarıyla ilişkili izinler düzenli olarak gözden geçirilmeli ve güvenlik risklerini engelleyecek şekilde doğru yapılandırıldığından emin olunmalıdır.
Savunmayı güçlendirmek için ek olarak:

- En az ayrıcalık (least privilege) prensibini uygulayın,
- Hassas kaynaklara erişimi sınırlayın,
- Anormal aktiviteleri yakalamak için güçlü izleme/denetim (monitoring) mekanizmaları kurun.

Bu adımlar, bu zafiyetlerden kaynaklanabilecek olası ihmal/yanlış yapılandırma risklerine karşı korumayı artırır.

TEKRARLAMA ADIMLARI

Yalnızca yetkili ve kontrollü bir ortamda, hedef AD CS sunucusu ve ilgili zafiyet sınıfı belirlenerek kurum içi güvenlik denetimi kapsamında doğrulama yapılabilir. Detaylı yönlendirmeler için referanslardaki teknik kaynaklar incelenmelidir.

REFERANSLAR

- **Active Directory Certificate Services'in Kötüye Kullanımı (Abusing AD CS)**
- **AD CS'yi Güvenli Hale Getirme: Microsoft Defender for Identity – Sensor duyurusu / güvenlik yaklaşımı**

ANALİZ

Analizimiz, en kritik pentest bulgularının arkasındaki temel nedenin hâlâ yanlış yapılandırmalar ve yama eksiklikleri olduğunu ortaya koyuyor. Endişe verici şekilde, tüm değerlendirmelerin yarısından fazlasında görülen ilk 3 bulgu; kolay erişilebilen araçlar ve temel teknikler kullanılarak bir kuruluşun ağının tamamen ele geçirilmesine yol açabiliyor. Bu saldırılar, çoğu BT ekibi tarafından genellikle fark edilmeden gerçekleşiyor; bu da geleneksel savunmalarda ciddi kör noktalar olduğunu gösteriyor.

YAPILANDIRMA ZAYIFLIKLARI

Yapılandırma zayıflıkları genellikle yöneticiler tarafından devreye alınan sistemlerde servislerin doğru şekilde "hardening" yapılmamasından kaynaklanır ve şu sorunları içerir: zayıf/varsayılan kimlik bilgileri, gereksiz şekilde dışa açılmış servisler veya aşırı kullanıcı yetkileri. Bazı yapılandırma zayıflıkları yalnızca sınırlı koşullarda istismar edilebilir olsa da, başarılı bir saldırının potansiyel etkisi genellikle yüksek olur.

YAMA EKSİKLİKLERİ

Yama eksiklikleri , kuruluşlar için hâlâ büyük bir problem olmaya devam ediyor ve genellikle uyumluluk/kompatibilite sorunları ile bazen de yama yönetimi çözümündeki yapılandırma problemlerinden kaynaklanıyor. Başarılı bir erişim; gizli verilere ve/veya sistemlere erişimle sonuçlanabilir.

Saldırganlar, kamuya açık araçlarla kolayca uygulanabilen yaygın yapılandırma hatalarını ve yama boşluklarını aktif olarak istismar ediyor. Bu zayıflıklar, çoğu zaman yetki yükseltme ve yetkisiz erişim için doğrudan bir yol sağlar; tehdit aktörlerinin kritik sistemlere hızlıca sızmasına ve kurum içinde yatay hareket etmesine (çoğu zaman tespit edilmeden) olanak tanır.

> Bu iki kritik sorun tek başına bile sık penetrasyon testinin gerekli olduğunu doğrular. Yıllık testlere güvenmek artık yeterli değildir; tehditler çok hızlı evrilmektedir. Süregelen otomatik pentest yaklaşımı, güvenlik açıklarına gerçek zamanlı görünürlük sağlayarak kuruluşların zafiyetler istismar edilmeden önce tespit edip gidermesine yardımcı olur.

Birçok kuruluş için zafiyet taraması (vulnerability scanning) yaygın bir uygulama olsa da, bu çözümler gerçek dünyadaki saldırı senaryolarında güvenlik risklerinin gerçek etkisini göstermekte yetersiz kalabilir. Örneğin Tenable'ın Nessus tarayıcısı LLMNR'yi yalnızca "bilgilendirici" bir konu olarak işaretleyebilir; ancak ciddi istismar potansiyelini yeterince yansıtmayabilir.

Nesil Teknoloji'i ile üç aylık veya aylık yapılan ağ penetrasyon testleri, yüzeysel tespitin ötesine geçer. Sadece zafiyetlerin varlığını ortaya koymakla kalmaz; aynı zamanda bu zafiyetlerin zincirlenerek (birleştirilerek) tam ölçekli bir ele geçirmeye nasıl dönüşebileceğine dair bağlam sunar. Böylece kurumlara, iş işten geçmeden önce anlamlı aksiyon almak için gerekli içgörüleri sağlar.

Nesil Teknoloji kuruluşların güvenlik risklerini gerçek zamanlı olarak proaktif şekilde azaltmasına ve ihlalleri önlemesine yardımcı olan lider bir bir sber güvenlik firmasıdır.Tespit edilen zafiyetleri, etkilerini ve bunların hem teknik hem stratejik olarak nasıl giderileceğini açıklayan; net ve aksiyon alınabilir raporlar sunar. Ayrıca uyum (compliance) çalışmalarını tutarlı ve denetime hazır sonuçlarla güçlendirir.

TEMEL ÖZELLİKLER & FAYDALAR

Kapsamlı KVKK Odaklı Değerlendirmeler Nesil Teknoloji olarak iç ağ + dış ağ + web uygulaması + API + bulut kapsamlarında pentest planlayıp uygularız. Kişisel veri işleyen kritik noktaların (VPN, AD, e-posta, yönetim panelleri, veri tabanları, dosya paylaşımları) uçtan uca incelendiğinden emin oluruz.

Gerçek Dünya Saldırı Senaryoları Testlerimiz, saldırganların gerçek hayatta kullandığı yöntemleri baz alan senaryolarla yürütülür. Böylece kurumun veri sızıntısı, yetkisiz erişim, hesap ele geçirme ve yatay hareket gibi risklere karşı hazırlık seviyesi net biçimde ortaya çıkar.

Net, Yöneticiye Uygun ve Aksiyon Odaklı Raporlama
Her bulgu için:

- Teknik detay + kanıt,
- Etki analizi (özellikle KVKK açısından kişisel veri riski),
- Önceliklendirme (kritik/yüksek/orta/düşük),
- Raporlarımız "denetime hazır" formatta, hızlı karar alınmasını sağlayacak şekilde hazırlanır

Sürekli Güvenlik İyileştirme
Tek seferlik test yerine, risk iştahına göre dönemsel (aylık/3 aylık/6 aylık) pentest ve doğrulama çalışmalarıyla güvenlik seviyesini sürekli güncel tutarız. Yeni açıklar ve değişen altyapı nedeniyle oluşan riskler erken yakalanır.

Hızlı İyileştirme ve Olay Müdahalesine Destek
Bulguların kapatılması sürecinde teknik ekiplere rehberlik eder; düzeltmeler sonrası yeniden test (re-test) ile doğrularız. Olası bir güvenlik olayı durumunda etkiyi azaltmaya yönelik hızlı teknik destek ve iyileştirme önerileri sağlarırız.

Uyumluluk ve Denetim Desteği
Pentest çıktılarımız, kurumların KVKK teknik tedbirleri başta olmak üzere aşağıdaki gereksinimlerle uyum çalışmalarını güçlendirir:

- ISO/IEC 27001 kontrolleri
- Sektörel regülasyonlar (kuruma göre)
- İç denetim / dış denetim için kanıt ve aksiyon planı üretimi

GÜVENLİĞİNİZİ BİR ÜST SEVİYEYE TAŞIYIN 2 KOLAY ADIMDA:

01

Web Sitemizi İnceleyin Hizmetlerimizi ve hedef odaklı pentest yaklaşımımızı inceleyin.

- www.nesilteknoloji.com

02

Hızlı Ön Görüşme / Keşif Alın Kapsam(iç ağ / dış ağ / web / API), kişisel veri temas noktaları ve risk önceliğini birlikte netleştirelim.

- www.nesilteknoloji.com

HAKKIMIZDA

NesilTeknoloji,kurumlarınKVKK ve veri koruma gereksinimlerine uygun şekilde siber risklerini azaltmasına yardımcı olan bir siber güvenlik danışmanlık firmasıdır. İç ağ, dış ağ, web uygulaması ve API

kapsamlarında yürüttüğümüz penetrasyon
testleriyle; yetkisiz erişim, veri sızıntısı, hesap ele geçirme ve yatay hareket gibi kritik riskleri ortaya çıkarırız.
Raporlarımız; teknik ekipler için uygulanabilir çözüm adımlarını, yöneticiler için ise risk/etki özeti ve önceliklendirilmiş aksiyon planını içerir. İyileştirmeler sonrası yeniden test ile bulguların kapatıldığını doğrularız.

www.nesilteknoloji.com

UZMAN EKİBİMİZLE SIZMA TESTİ ARTIK DAHA HIZLI.

www.nesilteknoloji.com