**ZAFİYETİN AÇIKLAMASI**
**Zafiyetin Adı:** Microsoft RDP Remote Code Execution Zafiyeti(Uzaktan Kod Çalıştırma Güvenlik Zafiyeti)
Ö**nem Dercesi**:Kritik
**CVE Puanı**:10

NSA araçlarının sızmasıyla birlikte MS17-010 zafiyet ve kodlarını takiben ortaya çıkan WannaCry ve Petya zararlıları pek çok kurumda hasara sebep olmuştu. Bu fidye zararlı yazılımlarının etkilerinin gölgesinde, Microsoft geçtiğimiz ay **CVE-2019-0708** koduna ve **BlueKeep** ismine sahip bir güvenlik açığı için yama çıkardığını duyurdu.
WannaCry fidye aracı kullanılarak Mayıs 2017 yılında dünya geneline hızla yayılan bir güvenlik açığı Windows XP ve Windows'un eski sürümlerini çalıştıran sistemleri sömürerek yayıldı. Microsoft, bu açıkla ilgili bir düzeltmeyi hızlıca yayınlasa da birçok eski ve savunmasız sistem güncellenmedi. Europol, WannaCry'ın 150 ülkede yaklaşık 200.000 bilgisayara yayıldığı tahmininde bulundu

**"WannaCry" tekerrürmü ediyor??**
Microsoft, tüm kullanıcılarını **WannaCry** benzeri bir saldırıya karşı kurban olmamaları için özellikle uyardı. Bulunan bu zafiyet, 2017 yılında gerçekleştirilen ve hala etkileri devam eden **WannaCry** saldırısına benzer bir saldırının başlangıç noktası olabilir.

Ayrıca 14 Mayıs tarihinde dikkat çeken bir güncelleme vardı. Bu güncelleme Keşfedilen bir güvenlik açığı olan Windows XP, Windows 7, Windows Server 2003, Windows Server 2008 R2 ve Windows Server 2008 sistemlerini etkileyen bir RDP zafiyeti idi. Bu zafiyet Windows 7, Windows Server 2008, ve Windows Server 2008 R2 sistemler dahil olmak üzere Windows'un desteklenen sürümlerinde yerleşik olarak gelen RDP (Uzak Masaüstü Hizmetleri) bileşeninde CVE-2019-0708 isimli bir zafiyet olarak tespit edildi. Microsoft'un uzun zaman önce güvenlik güncelleştirmelerini göndermeyi durdurduğu işletim sistemleri olan Windows XP ve Windows 2003 tarafından desteklenen sistemlerde de bu zafiyet bulunuyor.
**RDP** portu dış dünyaya açık eski bir işletim sisteminiz bulunuyorsa, bu zafiyet sizleri herhangi bir kimlik doğrulama olmaksızın saldırganlara uzaktan kod çalıştırmaya izin veren açık bir kapı haline getiriyor.

En çok göze çarpan zafiyet olarak Uzak Masaüstü Hizmetlerinde (eski adıyla Terminal Hizmetleri) bulunan CVE-2019-0708 numaralı kritik bir uzaktan kod çalıştırma güvenlik zafiyeti için Microsoft, tehlikeli güvenlik açığına yönelik herhangi bir saldırı kanıtı gözlemlenmediğini, ancak ciddi ve yakın bir tehdide neden olabileceğini belirtti.

Microsoft Security Response Center olay yanıt direktörü olan Simon Pope, "Henüz bu zafiyet ile ilgili bir exploit gözlemleyememiş olsak da kötü niyetli kişilerin bu güvenlik açığına yönelik yazılımlar ve programlar geliştirmesi olasıdır." dedi.

**Peki bu güvenlik açığı nasıl işliyor?**

Mevcut güvenlik açığı, RDP hizmetlerine gelen isteklerin, sistem tarafından işlenmesi esnasında karşılaştığı bir hatadan kaynaklanıyor. RDP kullanılarak özel olarak hazırlanmış istekleri sisteme gönderdiğinizde, uzaktan kod çalıştırma imkanına sahip olabiliyorsunuz. Güvenlik açığı, kullanıcıyla etkileşime gerek kalmaksızın kimlik doğrulamayı aşmanızı sağlıyor ve bu zafiyetten faydalanarak hedef sistemde kod çalıştırma, program yükleme; verileri görüntüleme, değiştirme veya silme yetkileriyle birlikte tam kullanıcı haklarına sahip yeni hesaplar oluşturabiliyorsunuz.

CVE-2019-0708, Microsoft'un en son çıkan; Windows 10 ,Windows 8.1, Windows 8 ,Windows Server 2019 ,Windows Server 2016, Windows Server 2012 R2 ve Windows Server 2012 işletim sistemlerini etkilemiyor.

Yukarıdaki sistemlerden herhangi birine sahip değilseniz Microsoft'un yayınladığı bu yamaları bir an önce edinmeniz gerekmektedir. Güncelleştirmeler, Uzak Masaüstü Hizmetleri'nin bu zafiyete neden olan bağlantı isteklerini işleme biçimini düzelterek bu güvenlik açığını gideriyor.

**Geçici Çözümler**

**1.** Gerekmiyorsa Uzak Masaüstü Hizmetlerini devre dışı bırakmak. Sisteminizde bu hizmetlere artık ihtiyaç duymuyorsanız hizmetleri devre dışı bırakabilirsiniz. Kullanılmayan ve gereksiz hizmetleri kapatmak güvenlik açıklarına maruz kalmanızı azaltmanıza yardımcı olacaktır.

**2.** Windows 7, Windows Server 2008 ve Windows Server 2008 R2'nin desteklenen sürümlerini çalıştıran sistemlerde Ağ Düzeyi Kimlik Doğrulamasını (NLA) etkinleştirin. Kimliği doğrulanmamış bir saldırgan güvenlik açığından faydalanarak sisteminize erişim sağlamak istediğinde NLA sayesinde kimlik doğrulaması ile karşılaşacaktır ve hesabınıza ait parolayı bilmiyorsa erişmesi mümkün olmayacaktır.

**3.** Güvenlik duvarınızdan 3389 numaralı TCP portunu engelleyin.Etkilenen sistemlerde 3389 numaralı TCP portu kullanılıyor. Bu bağlantı noktasına gelen istekleri güvenlik duvarınız ile engellemek, saldırganların buraya erişmesini engelleyecektir.

**Not:** Mevcut olarak sistemi exploit ettiği söylenen kodlar sürekli olarak Github gibi platformlarda ve forumlarda yayınlanmakta. Ancak yayınlanan kodlar ve programların bir çoğu tarafımızca incelendiğinde sistemleri crash edebilmekte veya programların içerisinde zararlı yazılımların bulunduğu tespit edilmekte. Zafiyetle ilgili kesin bir exploit aracı görseniz bile bu araçları tersine mühendislik yöntemleriyle analiz etmeden ve birkaç Sandbox üzerinde test etmeden çalıştırmamanızı öneriyoruz. Ek olarak, ilgili exploit aracını sanal makineler üzerinde çalıştırmanız daha sağlıklı olacaktır.

**İnceleme**

Bu güvenlik açığı ön kimlik doğrulamasını kullanıcı etkileşimine gerek kalmadan aşıyor. Başka bir deyişle, güvenlik açığı "wormable" bir durum ortaya çıkarıyor, yani bu güvenlik açığından yararlanan bir saldırgan herhangi bir yazılımı kullanarak savunmasız bilgisayarlardan bu güvenlik açığını barındıran bilgisayarlara yayılarak tıpkı 2017'de WannaCry'ın yaptığı şekilde bir yayılım gerçekleştirebilir. Böyle bir senaryonun

gerçekleşmesini önlemek için mümkün olan en kısa sürede sistemlere gerekli yamaların yüklenmesi gerekmektedir. Microsoft, şirketin bu açığa yönelik herhangi bir saldırı gözlemlemediğini ancak yakın bir zamanda ciddi bir tehlike oluşturabileceğini söyledi.

14 Mayıs tarihinde Microsoft tarafından BlueKeep adıyla duyurulan CVE-2019-0708 zafiyeti; Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows XP ve Windows Server 2003 versiyonlarını etkilemektedir." RemoteDesktopServices" hizmetinde uzaktan kod çalıştırma zafiyeti olarak tanımlanmaktadır. Giriş yapmasına yada sistemle herhangi bir etkileşime geçmesine gerek kalmadan istismar edilebilen **BlueKeep** zafiyetinin, bahsettiğimiz niteliklerinden ötürü MS17-010 gibi etkilerinin olabileceği Microsoft tarafından değerlendirilmektedir. Kritik altyapılar için yaygın kullanılan işletim sistemleri Windows 7 ve Windows 2008 R2 işletim sistemlerinin **BlueKeep** zafiyetinden etkileniyor olması,zafiyetin istismar kodunun geliştirilmesinin etkilerinin ne kadar büyük olabileceğini göstermektedir. Hali hazırda proof-of-concept (POC) kodları geliştirilmeye başlanmış olan BlueKeep zafiyetinin, 2019 yılı içerisinde Wanna Cry yada Petya gibi geniş çaplı bir saldırıya dönüşmesi kuvvetle muhtemeldir

**BLUE KEEP Zafiyet Tespiti**

https://www.rapid7.jp/db/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep adresinde yer alan metasploit modülü ile sistemlerinizin zafiyetli olup olmadığını kontrol edebilirsiniz.

https://github.com/zerosum0x0/CVE2019-0708

**Değerlendirme**

Güvenlik açığı, RDP hizmetinin gelen istekleri işleme biçimindeki hatadan kaynaklanmaktadır. Saldırgan, RDP hizmetine zararlı bir istek göndererek sistemi tetikler. Sonrasında zararlı istek hatalı şekilde işlendiğinden dolayı, istekte gönderilen zararlı kod sistem tarafından çalıştırmaktadır. CVE-2019-0708, kullanıcı etkileşimi gerektirmeyen bir güvenlik açığıdır bundan dolayı güvenlik zafiyetini başarıyla istismar eden bir saldırgan, hedef sistemde rasgele kod çalıştırabilmektedir. Bu çalıştırılan kodlar sayesinde de sisteme program yükleme, veri görüntüleme, değiştirme veya silme gibi sistem üzerinde değişiklikler yapabilmektedir. Aynı zamanda bu güvenlik zafiyetinden yararlanan herhangi bir zararlı yazılım, 2017'deki dünya genelinde 150 ülkede yaklaşık 200.000 bilgisayara yayılan WannaCry zararlı yazılımına benzer şekilde bütün savunmasız bilgisayarlara yayılabilecektir. Bu güvenlik zafiyeti, saldırganlara, internet'e bakan birçok Windows öğesinin çalışmasının muhtemel olduğu ortak bir saldırı vektörü sağlamaktadır. Shodan ve Binary Edge gibi platformlar sayesinde saldırganlar bu sistemleri kolaylıkla tespit edebilmektedir.

**Çözüm / Öneri**

Microsoft tarafından yayınlanan güvenlik güncellemelerinin; herhangi bir güvenlik olayı oluşmadan önce, tüm ilgili sunucularda acilen uygulanması gerekmektedir. Zafiyet tespit sistemleri kullanılarak tüm sistemler

bu güvenlik açığına karşı taranmalı ve tespit edilen sunucular bir an önce iyileştirilmelidir. Ek olarak, mümkünse güvenlik cihazlarında bu zafiyet ile ilgili imzaların devreye alınması faydalı olacaktır.

Sizlere önerimiz, gerekli yamaların acil olarak geçilmesidir. Windows 8 ve Windows 10 kullanıcılarının bu zafiyetten etkilenmediği için yapmaları gereken herhangi bir yama bulunmuyor.

CVE-2019-0708 için Microsoft, Windows 7, Windows Server 2008 ve Windows Server 2008 R2 için güncellemeler yayımlanmıştır. Ek olarak, Microsoft, Windows XP, Windows XP Professional, Windows XP Gömülü ve Windows Server 2003 dahil olmak üzere desteklenmeyen sistemler için de yamalar yayımlanmıştır. Bu güncellemeleri ivedilikle yüklemenizi veya RDP servisini kapatmanızı öneririz.

Windows 7, Windows 2008 ve Windows 2008 R2 için https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 üzerindeki yamaları uygulayabilirsiniz. Microsoft zafiyetin kritikliğinden dolayı desteğini bırakmasına rağmen Windows XP ve Windows 2003 içinde yama yayınladı, eğer bu tür sistemleriniz varsa **İlgili güncelleştime** kısmında yer alan link üzerinden gerekli güncellemeleri yapmalısınız

**BlueKeep** ile alakalı aktif olarak geliştirilen istismar kodlarından haberdar olmak için https://twitter.com/BlueKeepTracker botunu takip edebilirsiniz.

**Uyarı**:
Tüm sistemlere geçmeden önce, herhangi bir iş kesintisine neden olunmaması açısından güncellemeyi test etmenizi önermekteyiz.

**İlgili güncelleştime**

https://support.microsoft.com/en-ca/help/4500705/customer-guidance-for-cve-2019-0708

**Ek Bilgi(Referanslar):**

https://www.cvedetails.com/cve/CVE-2019-0708/
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708