# Uzaktan Çalışma Sırasında Kullanılan **Erişim Yöntemleri ve Zafiyetleri**

STM Cyber

STM

# Uzaktan Çalışma Sırasında Kullanılan Erişim Yöntemleri ve Zafiyetleri

Covid-19 pandemisiyle birlikte birçok kuruluş çalışma hayatının sürdürülebilmesi için uzaktan çalışma metoduna geçmek zorunda kaldı. Bu durum aynı zamanda çoğu şirket için ilk kez tümüyle ya da çoğunlukla uzaktan çalışma yapılacağı anlamına gelmektedir. Bilgisayar dünyasında uzaktan çalışma denildiğinde kurumlar tarafından en sık kullanılanılan teknolojiler VPN (Virtual Private Network) ve RDP (Remote Desktop Protocol)'dir. Günümüze kadar hackerların uzaktan çalışma için kullanılan bu teknolojiler üzerinde saldırı teknikleri geliştirdikleri ve birçok zafiyet buldukları bilinmektedir. Covid-19 pandemisiyle uzaktan çalışmanın bir anda dünya genelinde yaygınlaşması, çoğu saldırganın da atak vektörlerini yeniden bu teknolojilere kaydırmasına neden olmuştur.

Uzaktan erişim servisleri kontrol edildiğinde hem ülkemizde hem de Dünya genelinde en sık kullanılan 5 araç tespit edilmiş olup bu araçlar üzerindeki zafiyetler incelenerek Türkiye genelindeki dağılımlarından bahsedilmiştir. İlgili araçlar PulseSecure VPN, Fortinet VPN, Citrix ADC, Palo Alto Global Protect ürünleri olarak belirlenmiş, ek olarak RDP protokolü genelinde de bulunan zafiyetlere değinilmiştir. İlgili platformlara ait zafiyetlere ve istihbarat verilerine ulaşmak için hem açık kaynaklı veriler hem de STM tarafından geliştirilen siber tehdit istihbarat ürünü CyThreat platformu kullanılmıştır. İncelenen zafiyetlerin kapatılması için gerekli yamalar ve alınması gereken önlemlere ait öneriler de yazının devamında belirtilmiştir.

Araştırma sonucunda, uzaktan erişim araçlarında ve VPN sistemlerinde yüksek riskli birçok güvenlik açığının bulunduğu tespit edilmiştir. Bu zafiyetlerin senaryo ve hedefe bağlı olarak tek başına yalnızca hedefe sızmak için kullanılabileceği gibi, ilk önce hedef sisteme sızma daha sonrasında ise yatayda yayılmak için de zincirleme birleştirilerek kullanılabileceği de gözlemlenmiştir. İlgili zafiyetlerden etkilenmemek için servislerin ve ürünlerin en son versiyonda kullanıldığından her zaman emin olunmalıdır.

## ÜRÜN ZAFİYET VE TEHDİT ANALİZLERİ

## *Uzak Masaüstü Protokolü (Remote Desktop Protocol-RDP)*

Uzak masaüstü protokolü kısa adıyla RDP, bir bilgisayardan diğer bir bilgisayara ağ üzerinden bağlanıp uzaktan grafik arayüzü ile kontrol etmeyi sağlayan bir protokoldür. RDP protokolü Microsoft tarafından geliştirilmiş olup ilk olarak 1998 yılında çıkarılan "Microsoft NT 4.0 Terminal Server Edition" adlı işletim sistemi versiyonunda kullanmıştır. Bu versiyonla birlikte RDP servisleri Microsoft işletim sistemleri içerisine eklenmiş olup daha sonrasında çıkarılan tüm işletim sistemi versiyonlarında sistemle birlikte kurulu olarak gelmektedir. Ek bir lisans ücreti ve VPN ürünü satın alımı gibi ek maliyeti olmaması sebebiyle, büyük firmalar haricinde birçok küçük ve orta ölçekli firmalarda hem normal zamanda hem de Covid-19 salgını süresince RDP servislerini kullanmaktadır. İnternet üzerinde dışarıya açık RDP (port 3389) servisleri kontrol edildiğinde, 2020 yılı başlarından itibaren Covid-19 salgınının

başlamasıyla birlikte RDP servislerinde %127 artış olduğu görülmektedir. RDP servislerinin çok eski zamanlardan itibaren kullanılmaya başlanması sebebiyle, RDP protokolü üzerinde güvenlik araştırmacıları ve siber suçlular tarafından bulunan birçok kritik zafiyet bulunmaktadır.

RDP servislerine ait 2019 ve 2020 yılları içerisinde çıkarılan, risk skoru yüksek ve kritik değere sahip toplam 24 zafiyet tespit edilmiştir.

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 1 | Remote Desktop Services Remote Code Execution Vulnerability (Bluekeep) | CVE-2019-0708 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-0708 |
| 2 | Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability | CVE-2020-0610 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2020-0610 |
| 3 | Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability | CVE-2020-0609 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2020-0609 |
| 4 | Remote Desktop Services Remote Code Execution Vulnerability | CVE-2019-1181 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1181 |
| 5 | Remote Desktop Services Remote Code Execution Vulnerability | CVE-2019-1182 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1182 |
| 6 | Remote Desktop Services Remote Code Execution Vulnerability | CVE-2019-1222 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1222 |
| 7 | Remote Desktop Services Remote Code Execution Vulnerability | CVE-2019-1226 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1226 |
| 8 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2019-1290 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1290 |
| 9 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2019-1291 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1291 |
| 10 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2019-0787 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-0787 |
| 11 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2019-0788 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-0788 |

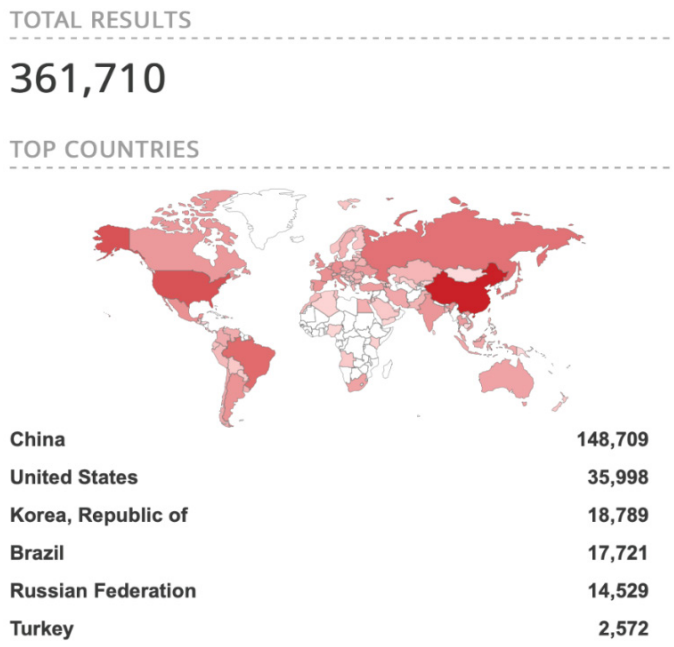
| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 12 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2020-0734 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2020-0734 |
| 13 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2019-1333 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-1333 |
| 14 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2020-0655 | 8 | https://nvd.nist.gov/vuln/detail/CVE-2020-0655 |
| 15 | Microsoft Windows RDP Network Level Authentication Bypass | CVE-2019-9510 | 7.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-9510 |
| 16 | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability | CVE-2019-1326 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-1326 |
| 17 | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability | CVE-2020-0660 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2020-0660 |
| 18 | Remote Desktop Protocol Information Disclosure Vulnerability | CVE-2019-1489 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-1489 |
| 19 | Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability | CVE-2019-1453 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-1453 |
| 20 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2020-0681 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2020-0681 |
| 21 | Remote Desktop Client Remote Code Execution Vulnerability | CVE-2020-0611 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2020-0611 |
| 22 | Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability | CVE-2020-0612 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2020-0612 |
| 23 | Remote Desktop Protocol Server Information Disclosure Vulnerability | CVE-2019-1224 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-1224 |
| 24 | Remote Desktop Protocol Server Information Disclosure Vulnerability | CVE-2019-1225 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-1225 |

*Tablo 1-Windows RDP Zafiyet Bilgileri*

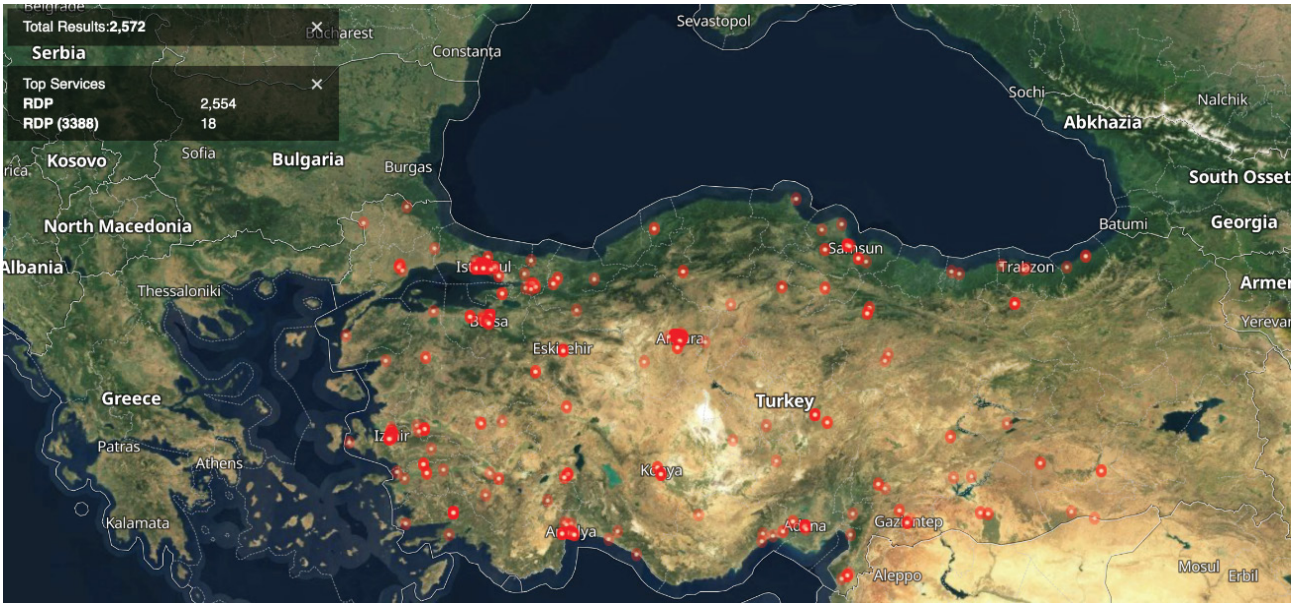
2019 yılından itibaren RDP servislerinde en çok istismar edilen kritik zafiyet Microsoft tarafından 14 Mayıs 2019'da bildirilen BlueKeep olarak da bilinen "CVE-2019-0708" zafiyeti olmuştur. Zafiyet, Remote Desktop Services (RDS) programının kodu içerisinde bulunan açıklık sebebiyle saldırganların uzaktan yetkili kullanıcı (NT Authority\System) haklarıyla komut çalıştırabilmesine olanak sağlamaktadır. Zafiyet herhangi bir kimlik

doğrulama işlemine ihtiyaç duyulmadan istismar edilebildiği için son derece kritik olarak sınıflandırılmakta ve 'wormable' (kendi kendine yayılabilen) özelliği sebebiyle de tehdit aktörleri tarafından sıklıkla kullanıldığı gözlemlenmektedir. Zafiyetten Windows 7, Windows 2008, Windows 2008 R2, Windows XP işletim sistemine sahip sistemler etkilenmektedir.

Dünya ve Türkiye genelinde **"CVE-2019-0708"** zafiyetine sahip sistemler kontrol edildiğinde dünya genelinde toplam 361,710 adet sistemin, Türkiye de ise toplam 2572 sistemin ilgili zafiyete sahip olduğu gözlemlenmiştir.




*Şekil 1-CVE-2019-0708 Zafiyetinin Dünya Genelinde Dağılımı*




*Şekil 2-CVE-2019-0708 Zafiyetinin Türkiye Genelinde Dağılımı*

Uzaktan erişim servisleri arasında yaygın olarak kullanılan RDP protokolü için özellikle yukarıda belirtilen ve uzaktan komut çalıştırmaya izin veren zafiyetleri gidermek için mümkünse Windows işletim sisteminin en güncel versiyonu kullanılmalı değilse de ilgili zafiyetler için yayınlanan güvenlik yamalarının uygulanıldığına emin olunmalıdır. BlueKeep zafiyeti için Microsoft tarafından yayınlanan yamaya ***https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 bağlantısından ulaşılabilir.***

Yamaların uygulanmasının yanı sıra olası saldırılardan ya da bu tarz çıkabilecek sıfırıncı gün zafiyetlerinden korunmak için ek olarak aşağıdaki önlemlerinde alınması önerilmektedir.

Uzaktan erişim gerekliliği bulunmayan sunucu ve istemciler üzerinde RDP servisi kapatılmalıdır. Ayrıca firewalllar üzerinde RDP'nin çalıştığı 3389 numaralı porta erişim, kurum dışındaki kişiler için engellenmelidir.

RDP üzerinde bulunan Ağ Seviyesinde Kimlik Doğrulama (Network Level Authentication) özelliği aktive edilmelidir. Bu özellik sayesinde RDP üzerinden bağlanmaya çalışan tüm kullanıcıların geçerli kullanıcı bilgileriyle giriş yapması gerekmektedir.

RDP üzerinden giriş yapma yetkisi olan tüm kullanıcıların parolalarının karmaşık olduğundan emin olunmalıdır. (En az 10 haneli ve büyük küçük harf ile özel karakter içeren parola kullanılması önerilmektedir.)

## *Citrix ADC*

Citrix ürünleri kişisel uygulamalar ve sunuculara uzaktan bağlanmanın yanı sıra kurumların ağ yönetimi içinde birçok servis ve ürün barındırmaktadır. Citrix uygulamalarının ve cihazlarının sağladığı bu servis, çalışanların uzaktan çalışma ve sistem yönetimi ihtiyaçlarını karşılarken, kötü niyetli tehdit aktörleri için de değerli bir erişim noktası olmaktadır.

Citrix teknolojilerinin 1989'dan beri yaygın olarak kullanılması sebebiyle ürün ve servisleriyle ilişkili birçok güvenlik açığı bulunmaktadır. Yapılan araştırmalar sonucunda uzaktan erişim sağlayan Citrix ADC servislerinde 2019 ve 2020 yılları itibariyle, risk skoru yüksek ve kritik değere sahip toplam 16 güvenlik açığı tespit edilmiştir.

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 1 | Citrix Application Delivery Controller/Gateway directory traversal | CVE-2019-19781 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-19781 |
| 2 | Citrix SD-WAN/Netscaler SD-WAN command injection | CVE-2019-12985 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12985 |

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 3 | Citrix SD-WAN/Netscaler SD-WAN command injection | CVE-2019-12986 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12986 |
| 4 | Citrix SD-WAN/Netscaler SD-WAN command injection | CVE-2019-12987 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12987 |
| 5 | Citrix SD-WAN/Netscaler SD-WAN command injection | CVE-2019-12988 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12988 |
| 6 | Citrix SD-WAN/Netscaler SD-WAN directory traversal | CVE-2019-12990 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12990 |
| 7 | Citrix SD-WAN/Netscaler SD-WAN command injection | CVE-2019-12991 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12991 |
| 8 | Citrix SD-WAN/Netscaler SD-WAN command injection | CVE-2019-12992 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-12992 |
| 9 | Citrix Application Delivery Controller/Gateway Management Interface weak authentication | CVE-2019-18225 | 8.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-18225 |
| 10 | Citrix SD-WAN Center/NetScaler SD-WAN command injection | CVE-2019-10883 | 8.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-10883 |
| 11 | Citrix SD-WAN/Netscaler SD-WAN sql injection | CVE-2019-12989 | 8.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-12989 |
| 12 | Citrix Workspace App Access Control privilege escalation | CVE-2019-11634 | 8.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-11634 |
| 13 | Citrix Application Delivery Management Access Control privilege escalation | CVE-2019-17366 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-17366 |
| 14 | Citrix Gateway privilege escalation | CVE-2020-10111 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2020-10111 |
| 15 | Citrix Netscaler Gateway/Application Delivery Controller memory corruption | CVE-2019-12044 | 7.4 | https://nvd.nist.gov/vuln/detail/CVE-2019-12044 |
| 16 | Citrix Storefront Server XML Data XML External Entity | CVE-2019-13608 | 7.4 | https://nvd.nist.gov/vuln/detail/CVE-2019-13608 |

***Tablo 2-Citrix ADC Zafiyet Bilgileri***

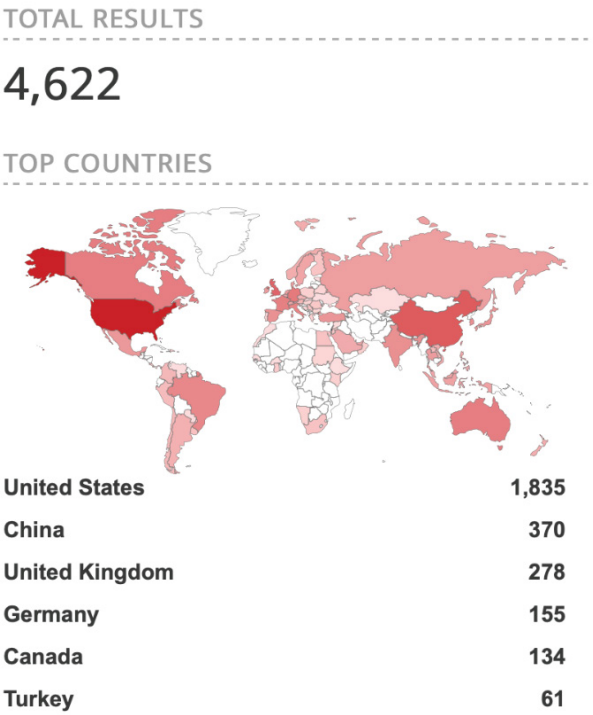
Bu zafiyetler içerisinde özellikle uzaktan çalışma metodunun yaygınlaşmasıyla birlikte daha sık istismar edilmeye başlanan zafiyet ise "CVE-2019-19781"dir. Bu zafiyet Citrix Application Delivery Controller (ADC) ve Citrix Gateway (NetScaler Gateway) bileşenlerinde yer almakta ve yama geçilmediği takdirde saldırganların kimlik doğrulaması yapmadan kolay bir şekilde kurum ağında kod çalıştırmasına olanak sağlamaktadır.

Bu zafiyetin yer aldığı Citrix sunucuları kurum ağında bulunmakta olduğundan ve kurumdaki tüm sunucu, iş istasyonları ve kritik sistemlere bağlanmak için kullanılması sebebiyle zafiyetin başarılı bir şekilde istismar edilmesi, tehdit aktörlerinin şirketin kritik uygulamalarına ve iç networkte bulunan kritik dosyalarına erişmesine sebep olmaktadır. Citrix tarafından bu zafiyet 17 Aralık 2019 tarihinde duyurulmuş olup aşağıdaki versiyonların zafiyetten etkilendiği bildirilmiştir.

- Citrix ADC ve Citrix Gateway versiyon 13.0
- Citrix ADC ve NetScaler Gateway versiyon 12.1
- Citrix ADC ve NetScaler Gateway versiyon 12.0
- Citrix ADC ve NetScaler Gateway versiyon 11.1
- Citrix NetScaler ADC and NetScaler Gateway versiyon 10.5

Citrix üzerinde bulunan **"CVE-2019-19781"** zafiyetinden etkilenmemek için kurumunuz bünyesinde Citrix'in en son versiyonunun kullanıldığından emin olunmalıdır.

Dünya ve Türkiye genelinde dışarıya açık ve bu zafiyete sahip sistemler kontrol edildiğinde Dünya'da toplam 4622 sistem, Türkiye'de ise 23 farklı organizasyonda toplam 61 cihaz olduğu tespit edilmiştir.




*Şekil 3-CVE-2019-19781 Zafiyetini Dünya Genelinde Yayılımı*

Genel olarak incelendiğinde dünya genelinde birçok saldırganın kurumlara kolayca sızmak için sıklıkla bu zafiyetten yararlandığı bu sebeple kurumunuza karşı olası yapılacak saldırılardan korunmak için en son versiona yükseltme işlemi yapılamıyorsa da **https://support.citrix.com/article/CTX267027** sitesinde yer alan yamaların uygulanması önerilmektedir.

Bu zamana kadar zafiyetten etkilenip etkilenilmediğinin tespit edilebilmesi için kurumlarda aşağıdaki adımların uygulanması önerilmektedir.

- Citrix sunucuları üzerinde zafiyetin istismar edildiğine dair bulguları control etmek için sunucular üzerinde bulunan "httpaccess.log" ve "httperror.log" dosyaları kontrol edilmelidir.
- Loglar içerisinde zafiyetin istismar edilmesi sırasında sıkça erişilmeye çalışılan "newbm.pl" ve "rmbm.pl" dosya kaynakları için "/vpns/" pathi içeren POST ve GET istekleri kontrol edilmelidir.
- Yine loglar içerisinde "GET /vpns/portal/<zararli_kod>" ifadesi geçen istekler kontrol edilmelidir.
- Anormal isimleri olan XML dosyalarına yapılan POST ve GET istekleri de loglar içerisinde incelenmeli, yukarıdaki bulgulardan birinin görülmesi halinde inceleme detaylandırılmalıdır.

Geriye dönük bazı log dosyaları boyutlarının büyük olması veya arşivleme politikası sebebiyle arşivlenmiş olabilir, arşivlenen log dosyalarının kontrolü de unutulmamalıdır.

## *Pulse Secure VPN*

Pulse Secure VPN kullanıcıların herhangi bir lokasyondan şirket sistemlerine çok faktörlü doğrulama ile güvenli bir şekilde bağlanmalarını sağlamaktadır. Yapılan araştırmalar sonucunda uzaktan erişim sağlayan Pulse Secure Connect VPN ürününe ait 2019 ve 2020 yılları itibariyle, risk skoru yüksek ve kritik değere sahip toplam 12 zafiyet tespit edilmiştir.

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 1 | Pulse Secure Pulse Connect Secure Permission File Upload privilege escalation | CVE-2019-11510 | 10 | https://nvd.nist.gov/vuln/detail/CVE-2019-11510 |
| 2 | Pulse Secure Pulse Connect Secure Session Hijacking weak authentication | CVE-2019-11540 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-11540 |
| 3 | Pulse Secure Pulse Connect Secure Applet tncc.jar weak authentication | CVE-2020-11580 | 9.1 | https://nvd.nist.gov/vuln/detail/CVE-2020-11580 |
| 4 | Pulse Secure Pulse Connect Secure/Pulse Policy Secure Admin Web Interface privilege escalation | CVE-2019-11509 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2019-11509 |
| 5 | Pulse Secure Pulse Connect Secure Applet tncc.jar privilege escalation | CVE-2020-11582 | 8.8 | https://nvd.nist.gov/vuln/detail/CVE-2020-11582 |

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 6 | Pulse Secure Pulse Connect Secure Applet tncc.jar Runtime.getRuntime().exec() privilege escalation | CVE-2020-11581 | 8.1 | https://nvd.nist.gov/vuln/detail/CVE-2020-11581 |
| 7 | Pulse Secure Pulse Connect Secure Session Token Replay weak authentication | CVE-2019-11213 | 8.1 | https://nvd.nist.gov/vuln/detail/CVE-2019-11213 |
| 8 | Pulse Secure Pulse Connect Secure SAML Authentication information disclosure | CVE-2019-11541 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2019-11541 |
| 9 | Pulse Secure Pulse Connect Secure Admin Web Interface directory traversal | CVE-2019-11508 | 7.2 | https://nvd.nist.gov/vuln/detail/CVE-2019-11508 |
| 10 | Pulse Secure Pulse Connect Secure Admin Web Interface command injection | CVE-2019-11539 | 7.2 | https://nvd.nist.gov/vuln/detail/CVE-2019-11539 |
| 11 | Pulse Secure Pulse Connect Secure Admin Web Interface Stack-based memory corruption | CVE-2019-11542 | 7.2 | https://nvd.nist.gov/vuln/detail/CVE-2019-11542 |
| 12 | Pulse Secure Pulse Connect Secure NFS privilege escalation | CVE-2019-11538 | 7.2 | https://nvd.nist.gov/vuln/detail/CVE-2019-11538 |

***Tablo 3-Pulse Secure Connect Zafiyet Bilgileri***

Geçtiğimiz yıl boyunca en çok bildirilen ve ürün ailesinde bulunan en kritik zafiyet, Pulse Secure tarafından ilk olarak 24 Nisan 2019'da yayınlanan ve Pulse Secure Connect VPN ürününü etkileyen ***"CVE-2019-11510"*** zafiyeti olmuştur. İlgili zafiyet sömürüldüğü takdirde saldırganlar sistem üzerinde bulunan sistem dosyası gibi kritik konfigürasyon dosyalarına kimlik doğrulamasına ihtiyaç duymadan erişebilmektedir. Bu zafiyet aynı zamanda diğer zafiyetlerle birlikte kullanılarak sisteme ilk sızıldıktan sonra içeride yetkili komut çalıştırma veya zararlı dosya yükleme gibi aktiviteler gerçekleştirilmesine olanak sağlamaktadır.

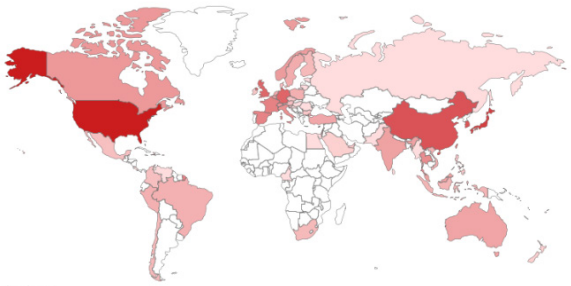
Örneğin, bir kullanıcı PulseSecure VPN uygulamasının admin arayüzüne giriş yaptığında, kullanıcının parolası şifrelenmemiş bir şekilde ***/data/runtime/mtmp/lmdb/data/data.mdb*** dizininde saklanmaktadır. Saldırgan, **"CVE-2019-11510"** zafiyetinin bulunduğu sistemlerde zafiyeti sömürerek yukarıdaki dizinde yer alan kullanıcı parolasına erişebilir. Elde ettiği kullanıcı bilgileriyle sisteme giriş yaptıktan sonra listede yer alan **"CVE-2019-11539"** zafiyetini kullanarak yetkili hesap haklarıyla komut çalıştırıp, sistemde zararlı aktiviteler gerçekleştirebilir. Alternatif olarak yine kullanıcının parolası ele geçirildikten sonra listede bulunan **"CVE-2019-11508"** zafiyeti kullanılarak dosya paylaşım alanına zararlı dosya bırakılarak yine sistemde zararlı aktiviteler gerçekleştirilebilir.

Dünya ve Türkiye genelinde **"CVE-2019-11510"** zafiyetine sahip sistemlere baktığımızda dünya genelinde 1175 sistemde zafiyetin bulunduğu Türkiye'de ise 10 adet sistemin zafiyetli sürüme sahip olduğu tespit edilmiştir.

TOTAL RESULTS

1,175

TOP COUNTRIES



| | |
|---|---|
| United States | 294 |
| Japan | 139 |
| China | 90 |
| Korea, Republic of | 87 |
| Germany | 60 |
| Turkey | 10 |

*Şekil 4-CVE-2019-11510 Zafiyetinin Dünya Genelinde Dağılımı*

Genel olarak incelendiğinde dünya genelinde birçok saldırganın ve devlet destekli saldırgan gruplarının kurumlara kolayca sızmak için güncel olarak sıklıkla bu zafiyetten yararlandığı görülmüştür.

2019 yılının Nisan ayında yaması çıkarılan zafiyet 2019 yılı içerisinde Ağustos ayında tamamen kapatılmıştır. Zafiyet bulunan ilgili Pulse Secure versiyon ve yamalı version bilgilerine aşağıdaki tablodan ulaşabilirsiniz. Zafiyetlerden etkilenmemek için her zaman Pulse Secure Connect ürününün en son versiyonunu kullanmalı, kurumda aşağıdaki zafiyetli versiyonlardan birinin kullanıldığı tespit edildiği takdirde ise acilen versiyonun en güncel versiyona yükseltilmesi, yükseltilemiyorsa da ilgili yamanın geçilmesi tavsiye edilmektedir. Zafiyetler ve yamaları hakkında detaylı bilgiye **https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101** sitesinden erişebilirsiniz.

| Zafiyetli Versiyon | Yama Versiyonu |
|---|---|
| Pulse Connect Secure 9.0RX | Pulse Connect Secure 9.0R3.4 & 9.0R4 |
| Pulse Connect Secure 8.3RX | Pulse Connect Secure 8.3R7.1 |
| Pulse Connect Secure 8.2RX | Pulse Connect Secure 8.2R12.1 |
| Pulse Connect Secure 8.1RX | Pulse Connect Secure 8.1R15.1 |

*Şekil 5- Pulse Secure Connect Zafiyetli Versiyonlar ve Yamalar*

Bu zamana kadar zafiyetten etkilenip etkilenilmediğinin tespit edilebilmesi için kurumlarda aşağıdaki kontrollerin yapılması önerilmektedir.

• Aşağıda verilen ağ indikatörlerinde yer alan IP adreslerinden veya kurumunuza bilinmeyen kaynaklardan gelen kimlik doğrulama logları kontrol edilmelidir.

**Ağ Indikatörleri**

| IP Adresi | IP Adresi | IP Adresi |
|---|---|---|
| 104.217.128.133 | 23.152.0.247 | 5.197.149.19 |
| 185.163.46.141 | 27.102.70.150 | 5.254.81.170 |
| 185.200.116.203 | 37.120.150.98 | 5.254.81.178 |
| 192.126.124.26 | 5.157.10.2 | 94.242.246.46 |

*Tablo 4- Pulse Secure Connect VPN Ağ Indikatörleri*

• Eğer Pulse Secure VPN ürünü kimliği doğrulanmamış isteklerin loglanması için konfigüre edildiyse aşağıdaki log örneğinde gösterildiği şekilde kuruma daha öncesinde yapılan saldırılar tespit edilebilmektedir.

**Info – [x.x.x.x] – System()[][] – 2020/05/02 09:15:26 – VPN-Remote – Connection from IP x.x.x.x not authenticated yet (URL=/dana-na/../dana/html5acc/guacamole/../../../../../../../data/runtime/mtmp/lmdb/randomVal/data.mdb?/dana/html5acc/guacamole/)**

## *Fortinet VPN*

Fortinet, şirket olarak geliştirdiği birçok güvenlik ürünün yanı sıra şirketlere uzaktan erişim için VPN, güvenli ağ geçidi ve kimlik ve erişim yönetimi araçları sağlamaktadır. Ürün ailesi içerisinde bulunan Fortinet VPN, çalışanların kurum sistemlerine ve kendi istemcilerine uzaktan şifrelenmiş olarak güvenli bir şekilde bağlanmasını sağlar. Yapılan araştırmalar sonucunda uzaktan erişim sağlayan Fortinet VPN servislerinde son 2 yılda risk skoru yüksek ve kritik değere sahip 3 güvenlik açığı tespit edilmiştir.

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 1 | Arbitrary File Read (Pre-Authentication) | CVE-2018-13379 | 9.8 | https://nvd.nist.gov/vuln/detail/CVE-2018-13379 |
| 2 | Improper Authorization (“Magic Backdoor”) | CVE-2018-13382 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2018-13382 |
| 3 | Heap Overflow (Pre-Authentication) | CVE-2018-13381 | 7.5 | https://nvd.nist.gov/vuln/detail/CVE-2018-13381 |

*Tablo 5-Fortinet VPN Zafiyet Bilgileri*

Fortinet VPN ürünü üzerinde son iki yılda en çok bildirilen ve sömürülen kritik zafiyet ise Fortinet tarafından ilk olarak 24 Mayıs 2019'da yayınlanan **"CVE-2018-13379"** olmuştur. Dünya ve Türkiye genelinde CVE-2018-13379 zafiyetine sahip sistemler kontrol edildiğinde taramalarımız sonucunda zafiyete sahip sistem bulunmamıştır.

Zafiyet sistem üzerinde kimlik doğrulaması yapmadan rastgele dizin gezme ve dosya okumaya olanak sağlamaktadır, bu sebeple birçok saldırgan tarafından hedef ağa sızmak için ilk etap olarak kullanılmaktadır. Araştırma sonucunda saldırganların genellikle zafiyet sayesinde VPN sisteminde bulunan ve içerisinde kullanıcı adı, parola bilgisini şifrelenmemiş şekilde saklayan **'ssl_websession'** adlı oturum dosyasını okudukları bu sayede kullanıcı bilgisini elde ettikleri tespit edilmiştir.

2019 yılının Eylül ayında ilk önce iki faktörlü kimlik doğrulaması çıkarılarak zafiyetin engellenmesi hedeflenmiş olup Kasım ayında çıkarılan yeni versiyon ile zafiyet tamamen kapatılmıştır. Zafiyet bulunan ilgili Fortinet FortiOS versiyonu ve yamalı versiyon bilgilerine aşağıdaki tablodan ulaşabilirsiniz. Zafiyetlerden etkilenmemek için her zaman Fortinet FortiOS ve SSL VPN ürününün en son versiyonunu kullanmalı, kurumda aşağıdaki zafiyetli versiyonlardan birinin kullanıldığı tespit edildiği takdirde ise acilen versiyonun en güncel versiyona yükseltilmesi, yükseltilemiyorsa da ilgili yamanın geçilmesi tavsiye edilmektedir.

| Zafiyetli Versiyon | Yama Versiyonu |
|---|---|
| FortiOS 5.4.1 to 5.4.10 | FortiOS 5.4.11 ve üzeri |
| FortiOS 5.6.0 to 5.6.8 | FortiOS 5.6.9 ve üzeri |
| FortiOS 6.0.0 to 6.0.4 | FortiOS 6.2.0 ve üzeri |

***Şekil 6- Fortinet Zafiyetli Versiyonlar ve Yamalar***

Bu zamana kadar zafiyetten etkilenip etkilenilmediğinin tespit edilebilmesi için kurumlarda eğer Fortigate cihazlarının web isteklerinin logları alınıyorsa veya önünde firewall gibi bir güvenlik cihazı varsa bu cihazların loglarından özelliklerine göre 'ssl_websession' dosyasının indirildiği kontrol edilerek tespit edilebilir, ayrıca 'ssl_websession' dosyasının boyutu ortalama 200 KB olması sebebiyle bu boyuttaki indirmelerde gözden geçirilerek yakalanabilir.

## *Palo Alto GlobalProtect*

Palo Alto GlobalProtect ürünü Palo Alto tarafından geliştirilmiş ağ güvenliği ve VPN istemci uygulamasıdır. 2020 yılı Nisan ayı itibariyle yapılan araştırmalar sonucunda Palo Alto GlobalProtect'i etkileyen, yüksek veya kritik olarak değerlendirilen 3 adet zafiyet tespit edilmiştir.

| No | Zafiyet Adı | CVE | CVSS v3 Risk Skor | Zafiyet Referans Uzantısı |
|---|---|---|---|---|
| 1 | Remote Code Execution in GlobalProtect Portal/Gateway Interface | CVE-2019-1579 | 8.1 | https://nvd.nist.gov/vuln/detail/CVE-2019-1579 |
| 2 | GlobalProtect Agent: Incorrect privilege assignment allows local privilege escalation | CVE-2020-1989 | 7.8 | https://nvd.nist.gov/vuln/detail/CVE-2020-1989 |
| 3 | Local Privilege Escalation in GlobalProtect Agent for Linux and Mac OS | CVE-2019-17436 | 7.1 | https://nvd.nist.gov/vuln/detail/CVE-2019-17436 |

*Tablo 6-Palo Alto GlobalProtect Zafiyet Bilgileri*

Bu zafiyetler içerisinde en kritik olarak göze çarpan zafiyet 17 Haziran 2019 tarihinde bir güvenlik araştırmacısı tarafından duyurulan ve 'format string' zafiyeti olarak da adlandırılan ***"CVE-2019-1579"***dir. Zafiyet, PAN SSL Gateway servisi üzerinde yapılan istemci/sunucu SSL el sıkışmaları sırasında cihazın belirli bir parametrede tutulan değişken değerini kontrol etmeden ve ayıklamadan ''snprintf'' fonksiyonuna göndermesi sonucunda oluşmaktadır. Saldırgan uzaktan herhangi bir kimlik doğrulama işlemi gerçekleştirmeden, ilgili parametrede tutulan değeri manipüle edecek şekilde özel olarak hazırladığı http isteğini, zafiyetli SSL VPN sistemine göndererek uzaktan kod çalıştırma işlemi gerçekleştirebilmektedir.

Dünya ve Türkiye genelinde araştırıldığında ilgili zafiyete sahip dışarıya açık sistem tespit edilememiştir. Zafiyete sahip olan Palo Alto GlobalProtect versiyonları aşağıda verilmiştir. Kurumlarda daima GlobalProtect ürününün en son versiyonunun kullanılması önerilmektedir. Kurumunuzda ilgili versiyonların kullanıldığı tespit edildiği takdirde ilgili yamanın acilen geçilmesi önerilmektedir.

| Etkilenen Versiyon | Yama Versiyonu |
|---|---|
| PAN-OS 7.1.18 and earlier | PAN-OS 7.1.19 and later |
| PAN-OS 8.0.11 and earlier | PAN-OS 8.0.12 and later |
| PAN-OS 8.1.2 and earlier | PAN-OS 8.1.3 and later |

*Şekil 7- Palo Alto GlobalProtect Zafiyetli Versiyonlar ve Yamalar*

İlgili yama versiyonlarına **https://security.paloaltonetworks.com/CVE-2019-1579** sitesinden ulaşıp sisteminizi en son versiyona yükseltebilirsiniz.

## *SONUÇ*

Yazı boyunca evden çalışırken en çok kullanılan uzaktan erişim teknolojileri ve bu teknolojilerde bulunan kritik zafiyetlerle, bu zafiyetlerin Dünya ve Türkiye genelinde nasıl bir dağılım gösterdiğinden bahsedilmiştir. Özellikle APT (Advanced Persistent Threat) olarak bilinen gelişmiş saldırı gruplarının yazıda bahsedilen zafiyetleri, diğer zafiyetlerle birleştirerek sistemlerde yayıldıkları ve hedef aldıkları organizasyonlardan kritik veri çalmak, fidye yazılımı dağıtmak gibi zararlı aktivitelerde bulundukları gözlemlenmektedir. İlgili zafiyetlerden etkilenmemek için daima kullanılan teknolojinin en son versiyonunun kullanılması, ek olarak yazı sırasında önerilen önlemlerin alınması önerilmektedir. Ayrıca uzaktan çalışma sırasında hem kurum olarak hem de bireysel olarak alınması gereken önlemler USOM tarafından da ***TR-20-159 (Güvenli "Uzaktan Çalışma" Kuralları)*** bildirisiyle yayınlanmış olup, bildiride yer alan öneriler yerine getirilerek kuruma ait atak yüzeyi minimum seviyeye indirilmelidir.