CVE-2019-19781

CVE-2019-19781 numaralı açıklık bildirimi ile ilgili, güncellemeler doğrultusunda Exclusive Networks Türkiye olarak müşterilerimiz için hazırlamış olduğumuz bilgilendirme yazısıdır.

GEÇMİŞ:

Geçtiğimiz aylarda Citrix sistemleri üzerinde, aktif olarak kullanılan bazı özellikler üzerinden saldırganların Citrix ADC, Citrix Gateway, Citrix SD-WAN cihazlara uzaktan erişerek code/ script/ command çalıştırabilmeye olanak sağlayan bir açıklığın bulunduğu tespit edilmişti.

Açıklık bildirimi CVE-2019-19781: https://support.citrix.com/article/CTX267027

Bu açıklığın ardından konuya ilişkin önlemleri kapsayan Mitigation Steps makalesi yayınlanmıştı.

Mitigation Steps: https://support.citrix.com/article/CTX267679

Daha önce gerçekleştirilmiş olabilecek saldırıların logları, cihaz üzerinde etkisi devam eden tanımlı işlemlerin kontrolü ve benzeri başlıklar için Citrix ve FireEye işbirliği ile bir inceleme aracı yayınlanmıştı. İlgili Forensic tool/ script* için erişim linkini aşağıda bulabilirsiniz.

*1.1 versiyonu geliştirilmiş ve script güncellenmiştir.

Citrix & FireEye Forensic Tool: https://www.citrix.com/blogs/2020/01/22/citrix-and-fireeye-mandiant-share-forensic-tool-for-cve-2019-19781/

Citrix geçtiğimiz günlerde ayrıca tüm Major sürümler için Fix içeren Firmware Build yayınlamıştır.

Citrix Final Fixed Version: https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/

GÜNCEL DURUM:

Son olarak, bu açıklık kullanılarak, kötü niyetli kişiler tarafından erişilmiş Citrix sistemlerinde bulunan Wildcard tipindeki sertifikalar da etkilenmiş olabilir. Citrix tarafından henüz resmi bir açıklama yapılmamıştır. Mitigation Steps olarak duyurulmuş konfigürasyon adımlarının uygulandığından, yamanın bulunduğu sürümde olduğumuzdan ve Forensic Tool ile kontrollerin yapıldığından emin olmanızı önermekteyiz.

Herhangi bir bulguya rastlanması halinde ve/ veya her ihtimale karşın sertifikanın yenilenmesi oluşabilecek risklerin önlenmesi adına faydalı olacaktır. Wildcard sertifikanızı yenilemek ya da olasılıkları değerlendirmek için sertifika sağlayıcınız ile iletişime geçmenizi öneririz.

Firmamız ile devam eden bir destek anlaşmanız varsa tüm sorularınız için Citrix_TR@exclusive-networks.com adresinden bize ulaşabilir ya da destek anlaşması yapmak için CitrixSales_TR@exclusive-networks.com adresine yazabilirsiniz.

ALINMASI GEREKEN AKSİYONLAR:

Forensic Tool kullanımı:

Forensic Tool da bulunan dosyayı Citrix üzerinde /var/tmp dizinine atalım, aşağıdaki şekilde çalıştıralım, ardından /tmp dizini altında aşağıdaki gibi results isminde bir dosya oluşturacak. Kontrol script kullanımı aşağıda paylaşılmıştır. Kullanım detayları için citrix_tr@exclusive-networks.com adresinden bilgi alabilirsiniz.

ioc-scanner-CVE-2019-19781:
https://github.com/citrix/ioc-scanner-CVE-2019-19781/

Management IP adresine SSH yapalım,
>Shell
#cd *<IOC-File-Dizin>*
#bash ioc-scanner-CVE-2019-19781.sh > "/tmp/results-$(date +"%m-%d-%Y-%T").txt"

Sonuç: /tmp dosyasında oluşacak, Örnek: results-02-04-2020-18:37:48.txt Olası riskin tanımında MATCH uyarısını ve hemen altında açıklamasını göreceğiz.

****
MATCH: blacklisted content 'exec[^u]'
Found evidence of potential compromise.
You should consider performing a forensic investigation of the system.
****
matches for 'exec[^u]':
///var/tmp/netscaler/portal/templates/.xml.ttc2

Versiyon güncellemesi:

11.1, 12.0, 12.1, 13.0, and Citrix SD-WAN 4000-WO, 5000-WO, 4100-WO, and 5100-WO

Sürümlerinde en son duyurulan Firmware/ Build'e hızlıca Upgrade önerilmektedir, sürüm güncellemesi sırasında Reboot olacağından, Standalone çalışan cihazlar için kesinti olacaktır. HA topolojide kesinti beklememekteyiz.

Standalone cihaz Upgrade:
https://docs.citrix.com/en-us/citrix-adc/13/upgrade-downgrade-citrix-adc-appliance/upgrade-standalone-appliance.html

HA cihaz Upgrade:
https://docs.citrix.com/en-us/citrix-adc/13/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-HA-pair.html

Upgrade konusunda bilgi almak ve destek talep etmek için citrix_tr@exclusive-networks.com adresine ulaşabilirsiniz.

Sertifika değişimi:

Forensic Tool çıktısı uyarınca gerekmesi halinde Sertifika yenilemek için sırasıyla yeni bir Certificate Key dosyası oluşturmalıyız, ardından gerekli bilgileri ekleyerek Certificate Signing Request dosyasını oluşturup Certifica Authority ile paylaşıp, yeni sertifikayı edinip Citrix üzerine yüklemeliyiz.

Sertifika oluşturma:
https://docs.citrix.com/en-us/citrix-adc/13/ssl/ssl-certificates/obtain-cert-frm-cert-auth.html

İşlem basamakları ve ekran görüntüleri için, citrix_tr@exclusive-networks.com adresinden bilgi alabilirsiniz.