NetScaler ADC ve NetScaler Gateway'deki CVE-2023-4966 ve CVE-2023-4967 Güvenlik Açıkları

Açıklama:

Zafiyetin sömürülebilmesi için önkoşul olan bir Ağ Geçidi (VPN sanal sunucusu, ICA Proxy, CVPN, RDP Proxy) veya AAA sanal sunucusu olarak yapılandırmış NetScaler ADC ve NetScaler Gateway cihazlarında CVE-2023-4966 ve CVE-2023-4967 güvenlik açıkları keşfedilmiştir. Güvenlik açıkları, NetScaler ADC ve NetScaler Gateway'in belirli istek türlerini işleme biçimindeki bir kusurdan kaynaklanmaktadır.

CVE-2023-4966 zafiyetinde kimliği doğrulanmamış bir saldırganın, kimliği doğrulanmış mevcut bir oturumu ele geçirmesi durumunda ele geçirilen hesabın izinlerine bağlı olarak kimlik bilgilerinin toplanabilmesi, yanal olarak hareket edilebilmesi ve ortamdaki ek kaynaklara erişim sağlanabilmesi gibi sonuçlara yol açabilir.

CVE-2023-4967 yüksek önemde bir hizmet reddi (DoS) güvenlik açığıdır. Bir saldırgan, cihazın CPU veya bellek gibi aşırı kaynak tüketmesine neden olacak bir istek göndermek için bu kusurdan yararlanabilir. Bu, aygıtın yanıt vermemesine veya çökmesine neden olabilir.

Etkilenen Versiyonlar:

NetScaler ADC ve NetScaler Gateway 14.1, 14.1-8.50 öncesi
NetScaler ADC ve NetScaler Gateway 13.1, 13.1-49.15 öncesi
NetScaler ADC ve NetScaler Gateway 13.0, 13.0-92.19 öncesi
NetScaler ADC 13.1-FIPS, 13.1-37.164 öncesi
NetScaler ADC 12.1-FIPS, 12.1-55.300 öncesi
NetScaler ADC 12.1-NDcPP 12.1-55.300 öncesi
Not: NetScaler ADC ve NetScaler Gateway sürüm 12.1 artık Kullanım Ömrü Sonu (EOL) durumundadır ve güvenlik açığına sahiptir.

Çözüm:

NetScaler ADC ve NetScaler Gateway 3.0-92.19 ve 13.0'ın sonraki sürümlerine yükseltin
NetScaler ADC ve NetScaler Gateway 13.1-49.15 ve 13.1'in sonraki sürümlerine yükseltin
NetScaler ADC ve NetScaler Gateway 14.1-8.50 ve sonraki sürümlerine yükseltin
NetScaler ADC 12.1-NDcPP 12.1-55.300 ve 12.1-NDcPP'nin sonraki sürümlerine yükseltin
NetScaler ADC 12.1-FIPS 12.1-55.300 ve 12.1-FIPS'in sonraki sürümlerine yükseltin
NetScaler ADC 13.1-FIPS 13.1-37.164 ve 13.1-FIPS'in sonraki sürümlerine yükseltin

CVE: CVE-2023-4966
CVSS Puanı: 9.4
Tanım: Hassas bilgilerin ifşa edilmesi

CVE: CVE-2023-4967
CVSS Puanı: 8.2
Tanım: Hizmet reddi (DoS)

NetScaler ADC: Citrix tarafından geliştirilen bir uygulama dağıtım denetleyicisidir.

NetScaler Gateway: Citrix tarafından geliştirilen bir ağ güvenliği ve erişim çözümüdür.

Referanslar:

https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967
https://www.tenable.com/blog/cve-2023-4966-citrix-netscaler-adc-and-netscaler-gateway-information-disclosure-exploited-in