T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Siber Olaylara Müdahale (SOME) Birimi

Güvenlik Özelliği Atlatma Zafiyeti

CVE-2019-1019

SOME GD. 19-05

02.07.2019

ZAFİYETİN AÇIKLAMASI
Zafiyetin Adı: Güvenlik Özelliği Atlatma Zafiyeti
Önem Derecesi: Kritik
CVE Puanı:6.5
Etkisi: Microsoft tarafından 11 Haziran 2019 tarihinde bir NETLOGON iletisinin oturum anahtarını alıp iletileri imzalayabilen ve bununla birlikte güvenlik özelliklerinin atlatılmasına imkân veren kritik bir zafiyet yayımlanmıştır.

Saldırgan bu güvenlik açığından yararlanmak için özel hazırlanmış bir kimlik doğrulama isteği gönderebilir, bazı güvenlik kısıtlamalarını atlamak ve yetkisiz eylemler gerçekleştirmek için bu sorunu kullanabilir. Bu şekilde başka atak denemelerinin olmasına da zemin hazırlanabilir.

CVE-2019-1019 kodlu bu zafiyeti istismar eden bir saldırgan bu güvenlik açığından yararlanmak için özel hazırlanmış bir kimlik doğrulama isteği gönderebilir. Bu güvenlik açığından başarıyla yararlanan bir saldırgan, orijinal kullanıcı ayrıcalıklarını kullanarak başka bir makineye erişebilir.

İşletim Sistemleri: Windows İşletim Sistemleri ve Uygulamaları

Çözüm Önerisi: Microsoft tarafından yayınlanan güvenlik güncellemelerinin; herhangi bir güvenlik olayı oluşmadan önce, tüm ilgili sunucularda ve istemcilerde acilen uygulanması gerekmektedir. Zafiyet tespit sistemleri kullanılarak tüm sistemler bu güvenlik açığına karşı taranmalı ve tespit edilen sunucular bir an önce iyileştirilmelidir.

Bu sorun güvenlik cihazlarında NTLM'nin ağ kimlik doğrulama mesajlarını doğrulama şeklini değiştirerek çözüldü. Tüm sistemlere güvenlik yaması geçmeden önce, herhangi bir iş kesintisine neden olunmaması açısından güncellemenin test edilmesi gerekmektedir.

Sürümler:
Windows 10, Windows 8.1, Windows 7, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019

Ek Bilgi (Referanslar):

https://www.symantec.com/security-center/vulnerabilities/writeup/108570
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1019
https://www.tenable.com/cve/CVE-2019-1019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1019
https://www.securityfocus.com/bid/108570
https://www.cvedetails.com/cve/CVE-2019-1019/
https://nvd.nist.gov/vuln/detail/CVE-2019-1019
https://threatpost.com/critical-microsoft-rce-bugs-windows/145572/

Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı / Siber Olaylara Müdahale (SOME) Birimi
Üniversiteler Mh. Dumlupınar Blv. 6001 Cd. No:9 Kat 3 Bilkent/Çankaya/ANKARA
Telefon No: +90 (312) 471 83 50 Birim E-Posta: some@saglik.gov.tr
İnt Adresi: https://some.saglik.gov.tr
Bilgi İçin: Esra ÖZÇELİK
Unvan: BİLGİSAYAR MÜHENDİSİ
E-Posta: esra.ozcelik@saglik.gov.tr