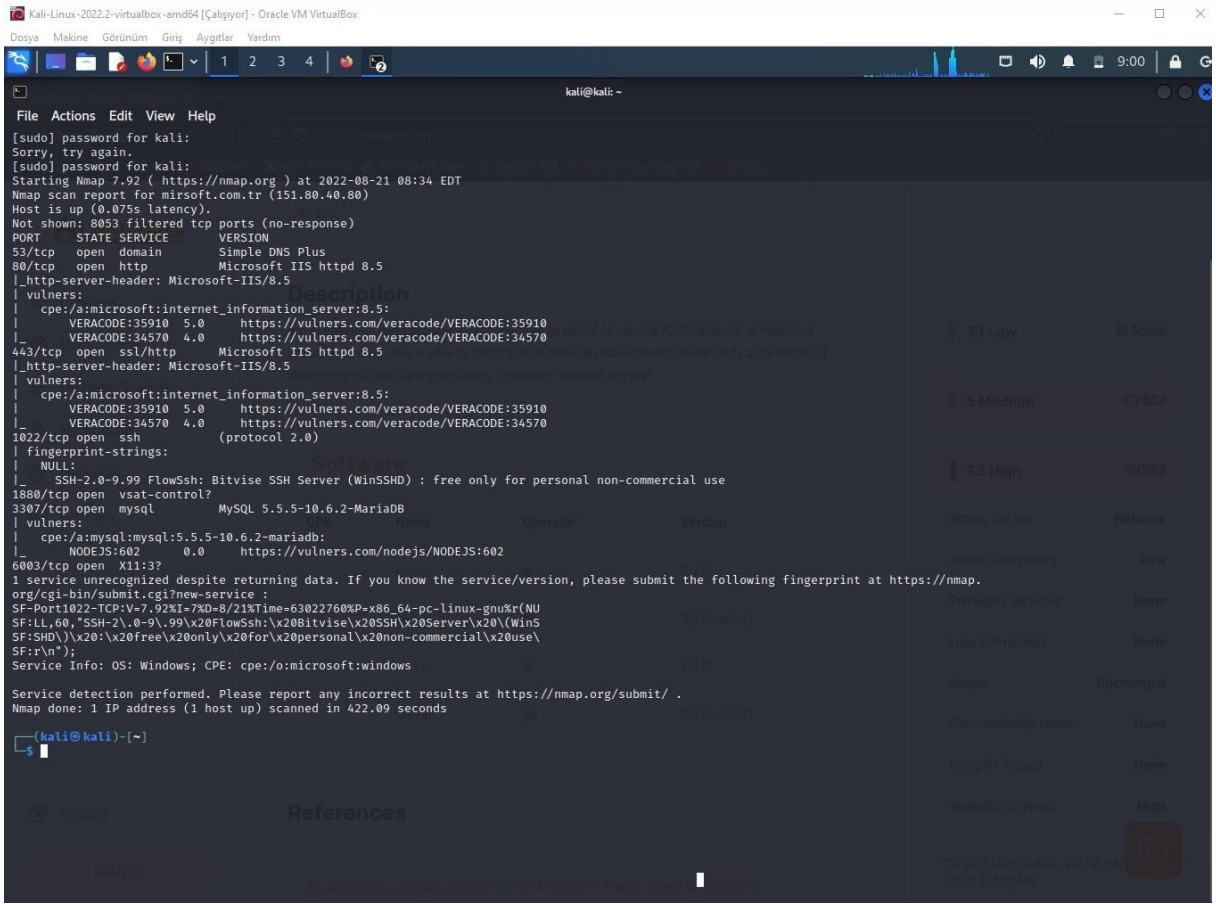
NMAP

BEN 170541065 NUMARALI GRUP2 ÜYESİ MİRAÇ GÖKATALAY.NMAP İLE MUSTSO.ORG.TR GÜVENLİK AÇIĞI TARAMASI YAPTIM VE BUNU NMAP GRUBU İLE PAYLAŞTIM.PAYLAŞIMLARIM AŞAĞIDA YER ALMAKTADIR.



Hizmet Reddi (DoS) Güvenlik Açığı

CVE-ID:CVE-2022-23712

Sunucu ,Hizmet Reddi'ne (DoS) karşı savunmasızdır.

Hizmet reddi (DoS) saldırısı, meşru kullanıcıların beklenen hizmetlere ve kaynaklara erişmesini engelleyen cihazlara, bilgi sistemlerine veya diğer ağ kaynaklarına yönelik bir siber saldırıdır.

Bu genellikle, hedef yanıt veremeyene veya kilitlenene kadar hedeflenen ana bilgisayarı veya ağı trafikle doldurarak gerçekleştirilir. DoS saldırıları, birkaç saatten birkaç aya kadar sürebilir ve kaynakları ve hizmetleri mevcut olmadığında şirketlere zaman ve paraya mal olabilir.

- Bir DoS saldırısında, sunucunun bant genişliğini aşırı yüklemek için hızlı ve sürekli çevrimiçi istekler hedef sunucuya gönderilir.

Öneri:

- İletişim, azaltma ve kurtarma dahil olmak üzere bir saldırıyı ele almanın tüm yönlerini kapsayan bir DoS yanıt planı oluşturun.
- Virüsten koruma ve kötü amaçlı yazılımdan koruma yazılımı yükleyerek ve gelen trafiği izleyen ve yöneten bir güvenlik duvarı kurarak ağ güvenliğinizi iyileştirin ve genel güvenlik duruşunuzu güçlendirin.
- Kötü niyetli trafiği filtreleyen ve yeniden yönlendiren ve bilinen saldırı imzalarını tespit edebilen bir DoS koruma hizmetine (izinsiz giriş tespit sistemi) kaydolun.
- Sistemleri ayrı alt ağlara ayırmak için ağ segmentasyonu eklemeyi düşünün ve tüm ağın taşmasını önleyin.
- Güvenlik ayarlarınızı ve uygulamalarınızı değerlendirin ve gerektiğinde iyileştirmeler yapın.

Ayrıcalık Yükseltme Güvenlik Açığı

Risk Seviyesi:Orta

CVE-ID:CVE-2022-23708

Sunucu Ayrıcalık Yükseltmesine karşı savunmasızdır.

Tanım

Güvenlik açığı, yerel bir kullanıcının sistemdeki ayrıcalıkları yükseltmesine olanak tanır.

Güvenlik açığı, uygulamanın Windows DWM Çekirdek Kitaplığı'nda güvenlik kısıtlamalarını gerektiği gibi uygulamaması nedeniyle oluşur ve bu da güvenlik kısıtlamalarının atlanmasına ve ayrıcalık yükselmesine neden olur.

Sunucu, ayrıcalık yükseltmeye karşı savunmasızdır. Saldırgan, güvenlik dizinindeki yerleşik korumaları devre dışı bırakarak geçerli dizine `*' dizin izniyle erişim sağlayabilir.

Bu güvenlik açığından yerel olarak yararlanılabilir. Saldırganın kimlik doğrulama bilgilerine sahip olması ve sistemde başarılı bir şekilde kimlik doğrulaması yapması gerekir

Güvenlik açığı bulunan yazılım sürümleri

Windows:: 10 - 11 21H2

Windows Sunucusu: 2019 – 2022

Öneri:

- Web sitesine güncellemeleri yükleyin.

Mysql Node.JS modülü uzaktan belleğe Maruz kalmaya karşı savunmasız

Risk Seviyesi:Düşük

Genel Bakış

BufferList , arabellekleri toplamanıza ve standart bir okunabilir arabellek arabirimiyle erişmenize izin veren bir kitaplıktır.

Bu paketin etkilenen sürümleri, Uzak Belleğe Maruz Kalmaya karşı savunmasızdır. Kullanıcı girişi consume() argümanla sonuçlanır ve negatif hale gelebilirse, BufferList durumu bozulabilir ve normal .slice() çağrılar yoluyla başlatılmamış belleği açığa çıkarması için kandırılabilir.

mysql2.14.0'dan önceki sürümler, bellek maruziyetini ortadan kaldırmaya açıktır.

Paketin etkilenen sürümleri, mysqlparola olarak bir numara sağlandığında ağ üzerinden başlatılmamış bir bellek ayırır ve gönderir.

Daha yeni node.js sürümlerinde eklenen bir atış nedeniyle yalnızca mysql6.0.0'ın altındaki Node.js sürümlerinde çalıştırma etkilenir.

Kavramın ispatı:

```
require('mysql').createConnection({
  host: 'localhost',
  user: 'user',
  password : USERPROVIDEDINPUT,  // number
  database : 'my_db'
}).connect();
```

Öneri:

Mysql 2.14.0 veya sonraki bir sürüme güncelleyin.