Eskişehir Osmangazi Üniversitesi
Bilgi İşlem Daire Başkanlığı
Siber Olaylara Müdahale Ekibi (SOME)

14.01.2025

Ağımızı Koruyalım!

Konu: Açık Kaynaklı VNC Sistemlerinde Tespit Edilen Güvenlik Açıkları Hakkında

Açıklama: Açık kaynaklı VNC yazılımlarında tespit edilen güvenlik açıkları; saldırganların sistemlere yetkisiz erişim kazanabilmesine veya uzaktan kod çalıştırarak kötücül yazılım kurabilmelelerine izin vermektedir.

(RealVNC, TightVNC, TurboVNC, LibVNC, UltraVNC)

ALINACAK ÖNLEMLER

VNC YAZILIMLARININ SİLİNMESİ

VNC protokolü ile erişim sağlanan sistemlerde yüklü olan VNC yazılımlarının sistemlerden kaldırılması

GÜÇLÜ PAROLALAR BELİRLEYİN.

VNC protokolü ile erişim sağlanan sistemlerde parola kullanılmaması veya boş/basit parola kullanılması durumunda parolaların boş/basit parola olmayacak şekilde değiştirilmesi.

ERİŞİM KISITLAMASI

VNC servisinin çalıştığı sistemlerde IP adresi bazlı tanımlamalar yapılarak kısıtlı kişilere erişim izni verilmesi

ANTİVİRÜS PROGRAMI KULLANIN.

Kişisel ve Kurumsal Güvenliğiniz için sistemlerde mutlaka antivirüs programı kullanınız.

Bu e-posta; **Kurumsal SOME Kurulum ve Yönetim Rehberinin "Kurum içi farkındalık çalışmalarının gerçekleştirilmesi" başlıklı 4.1.1 maddesi** uyarınca bilgilendirme amacıyla gönderilmiştir.

Güvenli çalışmalar diliyoruz.

SOME Ekibi

some.esogu.edu.tr
(Dahili No: 5204 / 5205 / 5235)