TÜBİMER
TÜBİTAK İLETİŞİM MERKEZİ

TÜBİTAK

GÖRÜŞ / ÖNERİ BAŞVURUSU

Başvuru Bilgileri

Başvuru Tarihi : 25.08.2022
Başvuru Numarası : 2208G1873

Başvuru Sahibi

TC Kimlik No	**:** 22733571022
Ad	**:** SADIK KAAN
Soyad	**:** GÜNDEM
E-Posta	**:** magnetar07@hotmail.com
Telefon	**:** 0 505 668 07 99
İl	**:** Antalya
İlçe	**:** Muratpaşa
Posta Kodu	**:** 07042
Adres	**:** Ücgen Mahallesi Tonguç Caddesi Bayram Duman Apartmanı 42/20 kat:6

Açıklama

Açıklama : https://talep.pardus.org.tr/browse/PYM-29020 "Merhaba, paylaştığımız dokümanda usb erişimini açıp kapatabilmek için yapılması gerekenler belirtilmiş. Badusb için kullanıcının şüpheli usb cihazını engellemesi için bir açılış betiği içerisine dokümandaki gibi ekleme yapması gereklidir. https://www.kernel.org/doc/Documentation/usb/authorization.txt Bununla ilgili ekibimiz tarafından en kısa zamanda donanım engelleyici uygulama yazılacaktır. Pardus ilginiz ve bildiriminiz için teşekkür ederiz." PYM-29020 numaralı destek talebimde 14.08.2022 tarihli 2208G1864 numaralı tubimer başvurumdaki belirttiğim husuları

ifade etmiştim. PYM-29020 talebinden gelen cevapta usb cihazının açılıp kapatılmasından ve donanım engelleyici modülden bahsedilmiştir. Esas konu donanımın engellenmesi veya usb cihazının açılıp kapatılması değildir. Tubimer başvurumda bahsettiğim gizli usb implantının ruber ducky ve usb ninja gibi basit bir "usb keyboard tabanlı bir badusb" değil kerneli ve sistem belleğini manipüle edebildiğini ve Kernel güvenliğini aşamadığı bilgisayarlarda ise kendisini farklı bir donanım olarak tanıttığını yazmıştım. Burada konu usb portların kendi busları değil usb buslarının bağlı olduğu PCI bridge grubunun kendisidir. Bu yüzden usb erişimini kapatmak problemi çözmez. Çünkü gizli usb implantı PCI Bridge I/O'sunu manipüle ederek kendini farklı PCI aygıtı olarak tanıtıp sisteme interrupt sinyali vermeye devam edecektir. Bir diğer esas konu ise gizli usb implantının verdiği interrupt sinyallerinin kerneli ve sistem belleğini manipüle edebilmesidir. Burada problem sadece donanımı engellemek değildir. Yetkisiz bir donanımın aşırı interrupt yüklemesi yaparak kerneli ve sistem belleğini etkilemesini engellemektir. Bu linux kernel güvenliği ile alakalı bir konudur.

Cevap Kanalı

Tercih Edilen Cevap Kanalı : Kısa mesaj
Sorumluluk metni'ni okudum ve kabul ediyorum : Evet