TÜBİMER
TÜBİTAK İLETİŞİM MERKEZİ

TÜBİTAK

GÖRÜŞ / ÖNERİ BAŞVURUSU

Başvuru Bilgileri

Başvuru Tarihi : 28.08.2022
Başvuru Numarası : 2208G1875

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 : 25.08.2022 - 11:00 tarihli 2208G1873 numaralı Tubimer başvurumda Problemin esas kaynağının USB busların kendisinde değil USB busların bağlı PCI bridge grubunun kendisinde olduğunu ve diğer problemin gizli usb implantının verdiği interrupt sinyallerinin kerneli ve sistemi manipüle edebildiğini ifade etmiştim. Talepte verilen çözüm önerisi olarak usb cihazlarının nasıl engelleneceğine dair kernel.org notu verilmiş ve donanım engelleyici bir modülün geliştirileceği ifade edilmiştir. USB cihazlarını usbcore.nousb=Y modülü ile GRUB komutu satırından engellemiştim zaten. Kernel yüklenirken [1.464737] usbcore: USB support

disabled sırasında usb cihazlar engelleniyor. Ama daha önceden USB busun bağlı olduğu PCI slotu [0.339472] pci 0000:02:00.3: [1022:15e0] type 00 class 0x0c0330 sırasında yüklendiği için sisteme gizlice sızıp kerneli ve sistem belleğini manipüle edebiliyor. Bahsettiğim gizli usb implantı ruber ducky ve usb ninja gibi sadece usb keyboard olarak hareket edip sisteme klavye tuşu olarak sinyal vermekle yetinmiyor. Bilgisayar açılırken kernele gizlice kod yükleyip sistemin kontrolünü ele geçiriyor.Kernel güvenliğini aşamadığı bilgisayarlarda sisteme aşırı interrupt yüklemesi yaparak bellek üzerinden sistemin kontrolünü ele geçiriyor. Benim pardus ekibinden isteğim linux kernel ekibi ve debian geliştirici ekibi ile iletişim kurup pci.c ve pci.h kaynak dosyasında tanımsız olarak duran pci_disable_device fonksiyonun kernel pci modülünün çalışan bir parametresi yapılmasını talep etmenizdir. Belirtilen PCI donanımları kernelde ilk sırada yüklendiği anda unregister ve disable işlemini yapılarsa gizli usb implantı sisteme sızamaz. Bu hususları değerlendirmenizi talep ediyorum. İncelemeniz için Pardus sistem raporu https://easyupload.io/x8l5ha

Cevap Kanalı

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