

main



Go to file

<> Code ▼

About

7-Zip through 21.07 on Windows allows privilege escalation and command execution when a file with the .7z extension is dragged to the Help>Contents area.

 [Readme](#)

 GPL-3.0 license

 Activity


☆ 684 stars

 26 watching

 104 forks

Report repository

 README

 GPL-3.0 license



INFORMATION

I haven't posted any poc code anywhere for privilege escalation attack. The poc codes found have nothing to do with privilege escalation. For your information.

7-zip hakkında

Releases

No releases published

Packages

No packages published

7-Zip, özgür ve ücretsiz bir dosya arşivleyicisidir. 7-Zip'in Komut İstemi sürümü Unix benzeri sistemler içinde düşünülmüş hatta AmigaOS bu saydıklarımıza dahil. Aynı zamanda DOS için de uyumlu Dost Portu için veya HX-DOS genişleticisi ile Windows komut İstemcisi'nde çalıştırılabilir.

CVE-2022-29072

Türkçe yazacağım biraz da siz Türkçe öğrenin.

Öncelikle zafiyeti bulma hikayeme değinmek istiyorum. WinRAR üzerinde XXE zafiyetini gerçekleştiren bir payload gördüm. Aynı zamanda HTML Helper dosyasının kullanarak javascript üzerinden ActiveXObject ve WScript.Shell sayesinde komut çalıştırmaya imkan sağlıyordu. Bunun lolbinlerde kullanılan HTA'dan hiç bir farkı yoktu olayı nasıl lehime dönüştürebileceğimi düşündüm.

(<https://www.exploit-db.com/exploits/47526>)

Aslında amacım 7z, zip, rar vb sıkıştırma teknolojilerinin uzantılarına çift tıkladıktan sonra hedef bilgisayar üzerinden reverse-shell alabilmektir bunun içinde HTML Helper dosyasını kullanabilir miyim diye düşünüyordum. WinAFL ile uzun fuzzing işlemleri sonrası FzGM.exe üzerinde heap-overflow olduğunu keşfettim fakat heap overflow sonrası yetkim yine aynı kullanıcı üzerinden olacağından bir anlamı da yoktu. Bu yüzden CreateRemoteThread kullanmadım çünkü API'i çağırmam gerekiyordu ve bu API'i tetikleyebilmek için bir chm dosyasına ihtiyacım vardı. Kaynak kodu incelediğimde özellikle iki yerde Windows API'ini çağırırken hatalı işlemler olduğunu farkettim ve bu direk yetkilendirme problemi yaratıyordu. Bu keşfetme noktam aşağıdaki resim de görüldüğü üzere FzGM.exe altında bir child process oluşturuyor. Normalde bu işlemin hh.exe üzerinde olmasını bekleriz.

Contributors 2



kagancapar Kağan Çapar

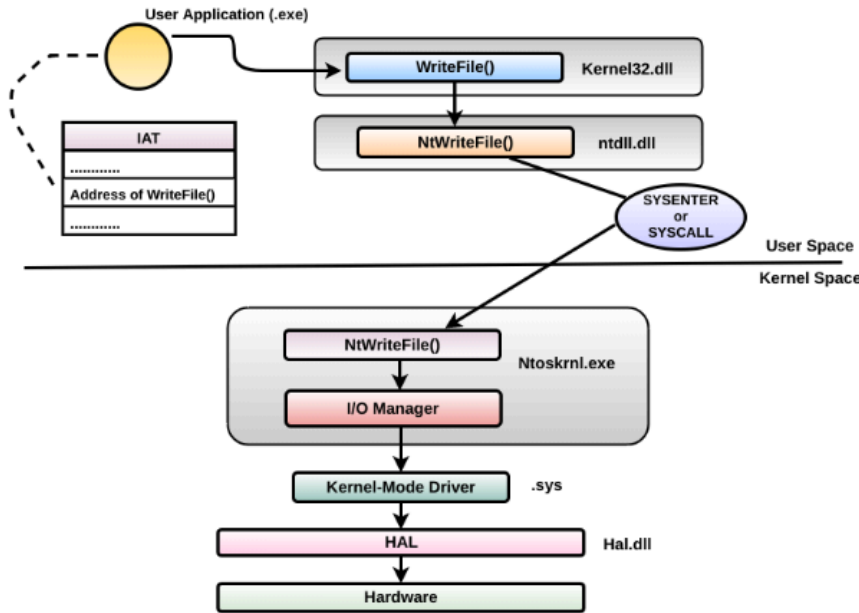


tsale Kostas

Languages

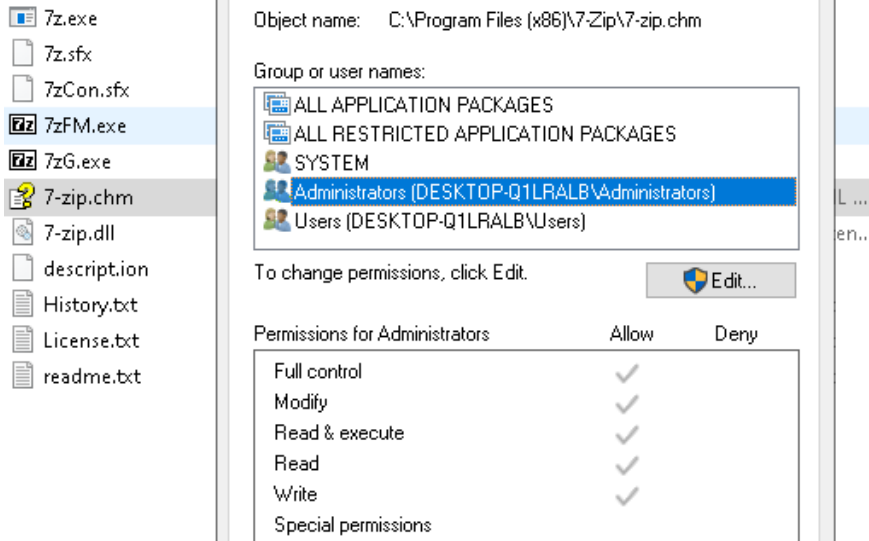
● HTML 100.0%

Process Name	7zFM.exe	1640	13.77 MB
Process Name	cmd.exe	12844	2.3 MB
Process Name	conhost.exe	3680	6.91 MB
Process Name	apimonitor-x64.exe	9284	0.43
Process Name	hh.exe	11720	12.25 MB
Process Name	cmd.exe	8484	2 MB
Process Name	conhost.exe	12456	6.96 MB

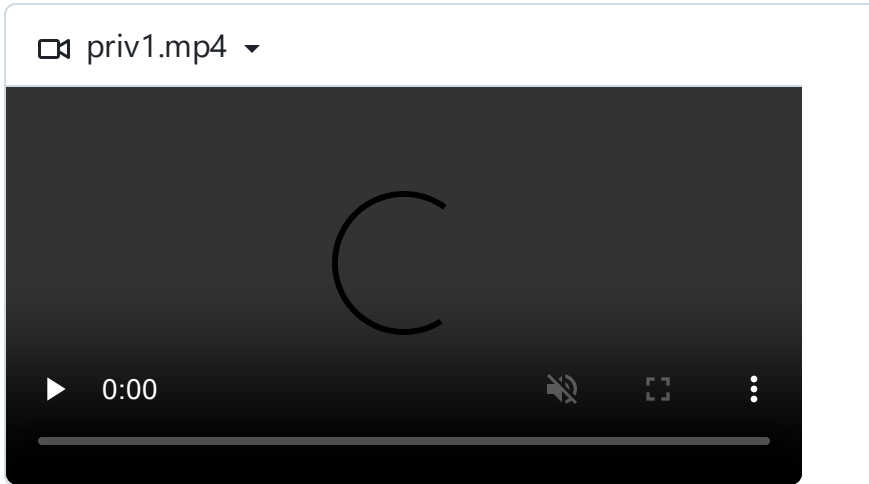


Eğer API'ı include etmeyip fonksiyon üzerinden doğru yapılandırma işlemi olsaydı hh.exe altında child process oluşturmasını beklerdim fakat 7-zip.chm dosyası bunu kendi üzerinden çağırılmaktadır tipik bir örneği 7-zip.chm dosyasını editleyip komut çalıştırma işlemi uygularsanız o zamanda görebilirsiniz. Heap overflow sonrası çağırılan API'nin yetkilendirme sorunu sonra 7z.dll dosyası içerisinde bulunan hatalı yapılandırmadan faydalandım ki bunun için uzun bir süredir uğraşıyorum. CreateRemoteThread() yapmanın bir anlamı yok. Benim payload'ın içerisinde çalıştırmam ve çağırmam gereken şey HTML Helper API'nin bizzat kendisi değil 7-zip üzerinden bu API'nin hook edildiği nokta ve o noktayı execute edebilmem fakat bu payload sadece hh.exe entegrasyonu ile çalıştığı için bu yüzden sürükle bırak gibi fonksiyon ile çalışmaktadır. 7-zip.chm dosyasının, 7-zip üzerinden HELP butonu ile çağırılması ve buraya çağırılan adresin payload içerisinde yetkilendirme sorunu görülen "base

pointer" yönlendirmem bizi bir üst kullanıcıya taşımaktadır. Buradan sonraki işlem ise payload'ın içerisinde psexec'in bulunması ve psexec -s cmd.exe komutuyla nt authority/system olarak system yetkisine yükselmesidir.



poc video:



ActiveXObject bypass hakkında

Soruların bir çoğu da ActiveX uyarısı üzerineydi bu problemin en temel şöyle giderebilirsiniz. Payload çalışmadan önce;

<'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0' -Name '1201' -Value '0' -PropertyType "DWord"> kontrol sağlamaktadır eğer bu değeri 1 ise popup ekrana gelmektedir şayet 0 olarak yeni bir değer atandıysa bypass edilmektedir. Fakat belirtmek gerekirse ki o an hangi user payload'ı çalıştırıyorsa onu etkilemektedir.

Önemli not

Ben gereken noktaları geliştiriciye söyledim ve CVE tarafından da bu kabul edildi. İnsanların kendini otorite zannetmesi ve onlara exploit'i vermem gerektiği gibi bir algı oluşmasına anlam veremiyorum. Ben zaten güncelleme sonrası yayınlayacağımı belirttiğim halde henüz update olmadan yapılan bu saygısızlık sanıyorum kendini otorite görmekten geçmektedir. Ben yetki yükseltme saldırısının poc kodunu hiçbir zaman yayınlamak istemeyebilirim bu benim hür irademdir ve bunun doğruluğu sorgulamak noktasında kimin ne düşündüğü ile zerre ilgilenmiyorum.

Alınabilecek önlem

Birinci yöntem: Eğer 7-zip güncelleme geçmezse 7-zip.chm dosyasının silinmesi gerçekleştirilebilir. İkinci yöntem: Program içerisinde yer alan tüm kullanıcılar read ve execute yetkisi ile erişim sağlamalıdır.

