

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Search

Sign in

Sign up

kagancapar / CVE-2022-29072

Public

Notifications

Fork 104

Star 684

<> Code

Issues 11

Pull requests

Actions

Projects

Security

Insights

main

Go to file

<> Code

kagancapar

Update README.md

76d8125 · 2 years ago

🕒 21 Commits

📁 command-exec-basic-7zip	Add files via upload	2 years ago
📁 privilege-escalation-7zip	Add files via upload	2 years ago
📁 xxe-basic-7zip	Add files via upload	2 years ago
📄 7z_CVE-2022-29072.yml	Create 7z_CVE-2022-29072.yml	2 years ago
📄 LICENSE	Initial commit	2 years ago
📄 README.md	Update README.md	2 years ago

📖 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

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 alabilmekti 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 çağırمام gerekiyordu ve bu API'i tetikleyebilmek için bir chm dosyasına ihtiyacım vardı. Kaynak kodu incelediğimde özellikle iki yerde Windows API'ını çağırırken hatalı işlemler olduğunu farkettim ve bu direk yetkilendirme problemi yaratıyordu. Bu keşfetme noktam aşağıdaki resim de

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

Releases

No releases published

Packages

No packages published

Contributors 2

kagancapar

Kağan Çapar

tsale

Kostas

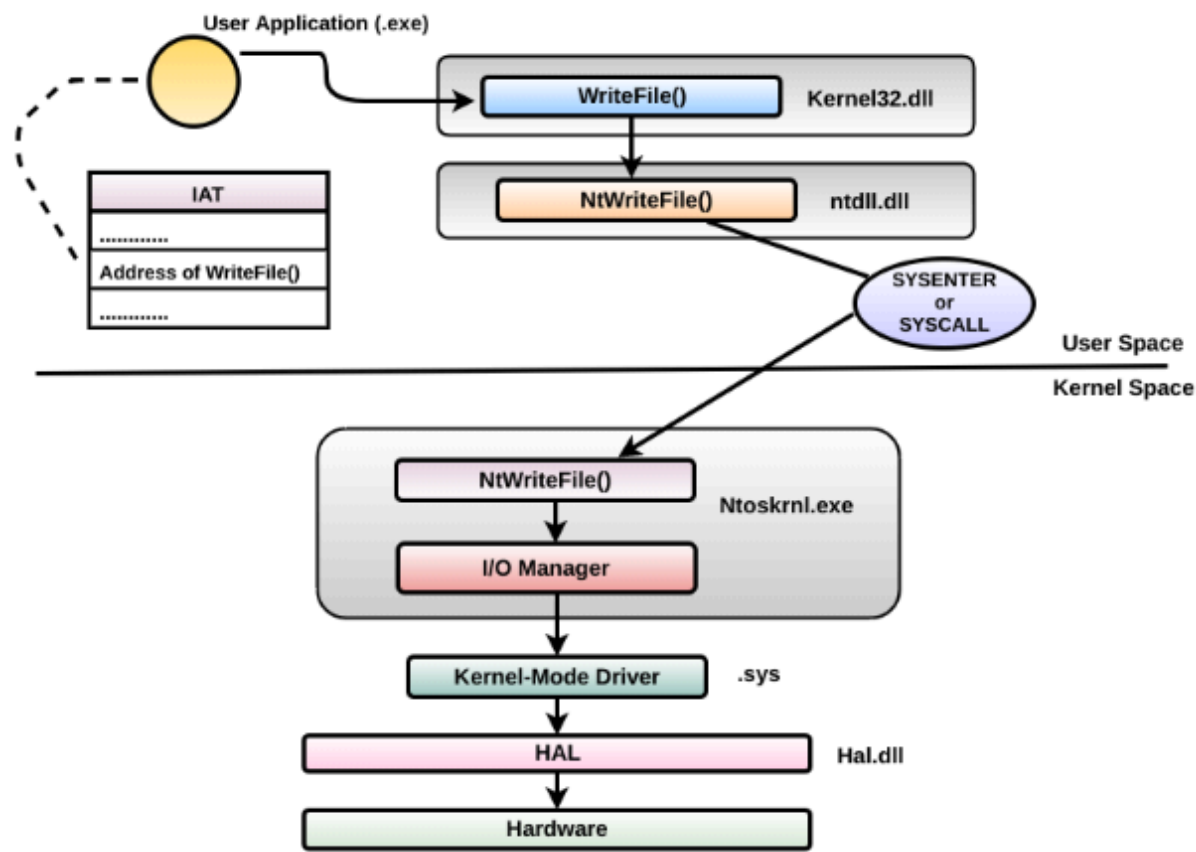
Languages

HTML 100.0%

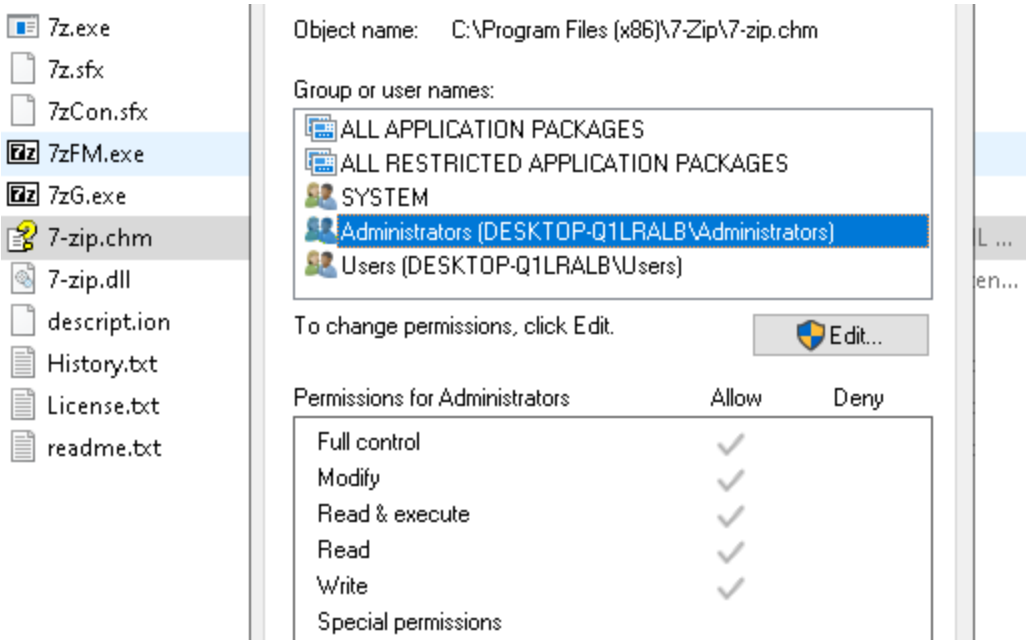
Page 1 of 3

görüldüğü üzere FzGM.exe altında bir child process oluşturuyor. Normalde bu işlemin hh.exe üzerinde olmasını bekleriz.

Process Name	PID	PPID	Working Set
7zFM.exe	1640	11720	13.77 MB
cmd.exe	12844	1640	2.3 MB
conhost.exe	3680	1640	6.91 MB
apimonitor-x64.exe	9284	0.43	12.32 MB
hh.exe	11720	1640	12.25 MB
cmd.exe	8484	11720	2 MB
conhost.exe	12456	11720	6.96 MB

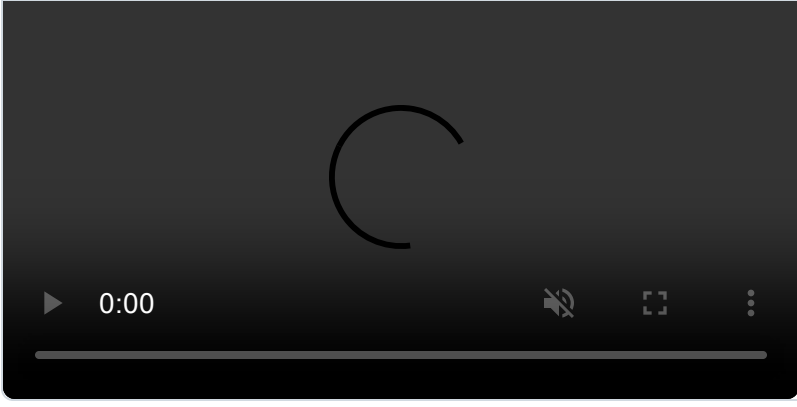


Eğer API'ı include etmeyip fonksiyon üzerinden doğru yapılandırma işlemi olsaydı hh.exe altında child process oluşturmasını beklerdim fakat 7-zip.chm dosyası bunu kendi üzerinden çağırılmaktadır tipik bir örneği 7-zip.chm dosyasını editleyip komut çalıştırma işlemi uygularsanız o zamanda görebilirsiniz. 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'ın bizzat kendisi değil 7-zip üzerinden bu API'ın hook edildiği nokta ve o noktayı execute edebilmem fakat bu payload sadece hh.exe entegrasyonu ile çalıştığı için bu yüzden sürükleyici 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:

priv1.mp4



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.

Sigma kuralı

İlgili sigma kuralı https://github.com/kagancapar/CVE-2022-29072/blob/main/7z_CVE-2022-29072.yml