T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Siber Olaylara Müdahale (SOME) Birimi

WinRAR'da keşfedilen ve potansiyel olarak 500 milyon kullanıcıyı etkileyen güvenlik açığı hakkinda bilgilendirme.

CVE-2018-20250

SOME GD. 19-03

20.03.2019

ZAFİYETİN AÇIKLAMASI
Zafiyetin Adı: WinRAR'da keşfedilen ve potansiyel olarak 500 milyon kullanıcıyı etkileyen güvenlik açığının yarattığı tehdit...
Önem Dercesi:Yüksek
Cvss puanı:7.8

WinRAR dünya genelinde 500 milyondan fazla kullanıcıya hitap eden, dünyanın popüler sıkıştırma aracıdır.

CVE-2018-20250 olarak izlenen güvenlik açığı Şubat'ta Check Point'teki uzmanlar tarafından keşfedildi, bir saldırganın hedef sistemin kontrolünü ele geçirmesine izin veriyordu. keşfedilen WinRAR ACE kod enjeksiyon güvenlik açığı WinRAR **UNACEV2.DLL** kütüphanesinde bulunuyor.

Yazılım açıkları, saldırganların etkilenen makineye uzaktan komutları uygulamak için istismar kitlerini kullanmalarına izin veren hatalardır. Bu, eğer yüklü olmayan bir yazılımın yüklü olması durumunda, bilgisayar korsanlarının sisteminize kötü amaçlı yazılım yüklemek için hatayı kötüye kullanabileceği anlamına gelir.

Yeni güvenlik açığımız olan **JNEC.a** Sıkıştırılmış RAR dosya arşivinde depolanan Fidye yazılımıdır. Bu arada, arka planda JNEC.a Ransomware kurbanın sistemine düşer ve dosyaları şifrelemek ve sistemi kilitlemek için işlemlerine başlar. Güvenlik açığı, **JNEC.a** kötü amaçlı yazılımının yürütülebilir **GoogleUpdate.exe** dosyasını Windows Başlangıç klasörüne yerleştirmesini ve böylece kötü amaçlı programın işletim sistemi her başlatıldığında başlatılmasını sağlar.

Virüs totalda 29 antivirüs tespit edildi ve **JNEC.a**'yı tehdit olarak algıladı.

360 Threat Intelligence Center'dan araştırmacılar ilk olarak bu **JNEC.a Ransomware** örneğini **(vk_4221345.rar)** dosya adıyla ortaya çıkardılar.

Şifreleme prosedürü dosyayı kilitlemeye başlar ve fidye notlarını görüntüler ve şifre çözme anahtarını kurtarma adımlarını sıralamaya başlar. Fidye yazılımı kurbanın bilgisayarındaki dosyaları şifreledikten sonra, fidye ödeyeceklerinde dosyanın şifre çözme anahtarını almak için mağdurların oluşturması gereken bir Gmail adresi tanımlanır. Fidye yazılımı kurbanın makinesindeki verileri şifreler ve fidye olarak 0.05 bitcoin (yaklaşık 200 $) isteyen şifreli veri **.Jnec** uzantısını ekler.

JNEC.a Ransomware ayrıca ödemenin nasıl yapılacağına ilişkin talimatlar sağlamak için virüslü bilgisayarda bir fidye notu (**JNEC.README.TXT**) düşer.

JNEC.a .NET programlama dilinde yazılmış, kötü amaçlı bir yazılım olup yayılması için WinRAR güvenlik açığından yararlanır.

Tehdite konu olan durumlar ise, kişisel resimleri, veritabanlarını, belgeleri, elektronik tabloları ve diğer dosyaları kapsamlı bir şekilde kilitlemek için karmaşık bir şifreleme algoritması kullanılması ve ardından kullanıcıların PC'de bulunan verileri çalıştırmasını engelleyen bir **.Jnec** uzantısı eklenmesidir.

Bununla birlikte, **JNEC.a** virüsünün derinlemesine araştırılması sonucu fidye yazılımının yazarlarından olan Güvenlik araştırmacısı Michael Gillespie'in analizine göre bu fidye yazılımında var olan hata nedeniyle, kimse (fidye yazılımın geliştiricisi bile) bu dosyanın şifresini çözemez bu yüzden fidye ödemenin tamamen anlamsız olduğunu ifade etmiştir.

İzlenebilecek yollar

Tüm WinRAR kullanıcılarının en güncel sürümü kullanmaları tavsiye edilir.

Kötü amaçlı yazılım yazarlarının güvenlik açıklarından yararlanmasını önlemek için bilgisayar kullanım rutininize yazılım güncellemeleri ekleyin.

Kötü amaçlı yazılım geliştiricileri tarafından sömürülme riski, aynı zamanda istenmeyen hatta kötü amaçlı programları barındıran sahte güncelleme sitelerinde de mevcut olduğundan dolayı bu sitelere girilmemesi tavsiye edilir.

Kapsamlı bir antivürüs yazılımının kurulu olması zorunludur, çünkü gelen tehditlere karşı kullanıcıları uyarır ve makineye bulaşmasını önler.
Ne yazık ki, JNEC.a virüsünün kilitli olduğu dosyaları almak için hazır bir yedeğiniz yoksa çok az şansınız vardır.

Verilerinizin en azından bir kısmının kurtarılması, üçüncü taraf yazılımların yardımı ile mümkün olabilir.

Genel bir kural olarak da güvenilir bir kaynaktan geldiğine emin olmadığınız dosyaları asla açmayınız.

Çalışanlar zip, rar ve benzeri arşiv dosyaların tehlikeli olabileceği konusunda bilgilendirilmelidir.

Kaynağını bilmediğiniz yerlerden gelen e-posta ekinde zip, rar ve benzeri sıkıştırılmış dosyalar varsa, e-posta güvenlik çözümünüz tarafından engellendiğini kontrol edin.
Arşiv dosyalarını dışarı çıkarttıktan sonra programı çalıştırmadan önce güncel bir antivirüs ile dosya virüs taraması yapılması gerektiğini unutmayın.

Virüsü özetlersek:
İsim: JNEC.a
Tür:Ransomware
Programlama dili: .NET
İlişkili dosyalar: GoogleUpdate.exe, JNEC.A.exe, vk_4221345.rar, iku_m2VtkXA.jpg
Fidye notu: JNEC.README.TXT
Zafiyet: 19-year old WinRAR vulnerability
Fidye miktarı: 0.05 BTC
Şifrenin çözülmesi mümkünmü: fidye ödense bile kötü amaçlı yazılım yazarıda dahil olmak üzere hiçkimsenin verilerin şifresini çözmesi mümkün değil.
Önlem: Kötü amaçlı bu yazılımı tanıyabilecek güvenlik yazılımı kullanın.
Kurtarma: Virüs hasarlarından kurtulmak için PC'nizi Reimage ile tarayın

Çözüm Önerisi: Bu açıktan etkilenmemek için enaz WinRAR 5.70 ve üzeri sürümü yüklemelisiniz. Güncellemeyi winrar resmi hesabından yapabilirsiniz.
https://www.rarlab.com/download.htm

Ek Bilgi(Referanslar):

1-https://gbhackers.com/jnec-a-ransomware/
2-https://www.cwenterprises.co.uk/alert-hackers-launching-new-jnec-a-ransomware-via-winrar-exploits-do-not-pay/
3- https://securityaffairs.co/wordpress/82606/malware/jnec-a-ransomware-winrar.html
4- https://www.facebook.com/cybercuremecom/
5- https://www.2-spyware.com/remove-jnec-a-ransomware.html
6- https://brica.de/alerts/alert/public/
7-www.feedspot.com/infiniterss.php?q=site:https%3A%2F%2Fgbhackers.com%2Ffeed
8-www.virustotal.com/gui/file/
9-https://riskdiscovery.com/
10-https://www.rarlab.com/download.htm
11-https://nvd.nist.gov/vuln/detail/CVE-2018-20250#vulnCurrentDescriptionTitle