HAVELSAN DIGITAL

Think Future

SİBER GÜVENLİK BÜLTENİ

KASIM 2021

SİBER GÜVENLİK DİREKTÖRLÜĞÜ

www.HAVELSAN.com.tr

HAVELSAN
DIGITAL

Yamasız Yetkisiz Dosya Okuma Zafiyeti

Feyzi Yuşa KARABABA
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

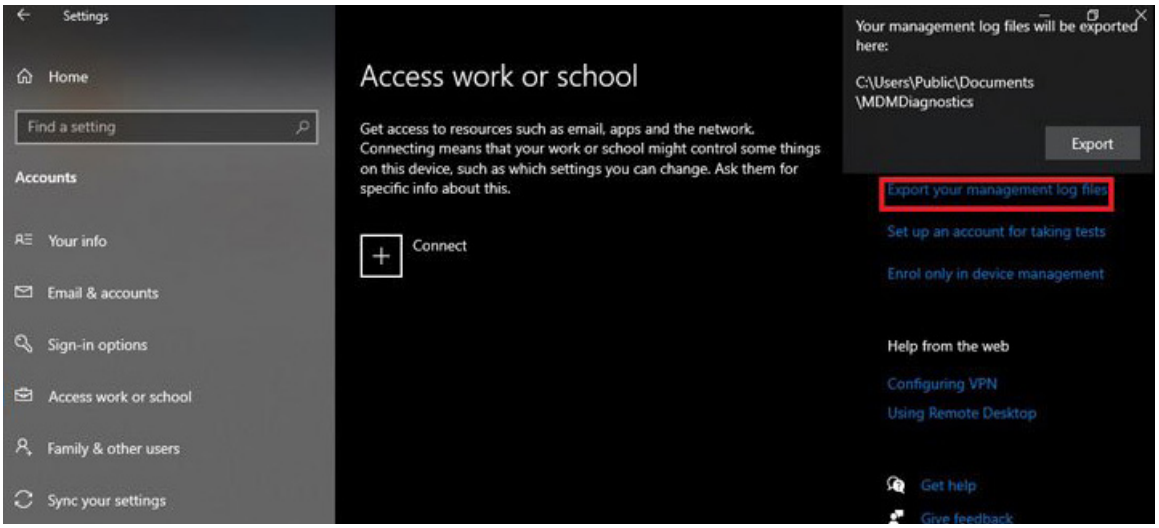
Yamasız Yetkisiz Dosya Okuma Zafiyeti

Zafiyet Genel Bilgi

Windows'un tam olarak kapatamadığı, zafiyetli sistemlerde bilgi ifşasına ve yerel ayrıcalık yükseltilme (Local Privilege Escalation(LPE)) yetkisine izin veren zafiyet için gayri resmi yamalar yayımlandı.

CVE-2021-24084 (CVSS puanı 5.5) ile kayda geçen zafiyet, Windows Mobile Aygıt Yönetimi'nde, bir saldırganın yetkisiz bir şekilde dosya sistemine erişmesine ve rastgele dosyaları okumasına olanak sağlamaktadır.

"Abdelhamid Naceri" adındaki siber güvenlik araştırmacısı tarafından Ekim 2020'de keşfedilen zafiyetin, Şubat 2021 de yayımlanan güncelle ile kapatılması istendi ancak Haziran 2021'de araştırmacı tarafından tekrar gözlemlendiğinde, güncellemenin eksik ve tam yapılamadığını, bu yama ile hali hazırdaki açığa ek olarak ayrıcalık yükseltme zafiyetinin ve zararlı kod çalıştırmaya imkan sağladığını keşfetti. Windows 10 kullanan ve son güncellemeyi alan tüm cihazlarda bu zafiyet mevcut.



Ancak güvenlik açığının kullanılabilmesi için C: sürücüsünde sistem koruma özelliğinin etkinleştirilmiş ve bilgisayarda en az bir yerel yönetici hesabının olması gerekmektedir. Bu zafiyetten sadece "Windows 10" cihazlar etkilenmektedir.

Bu zafiyet, Microsoft tarafından yayınlanan eksik yapılandırılan güncellemeler ile ortaya çıkan bilinen üçüncü sıfırıncı gün açığı oldu.

Etki Alanı

Windows 10 işletim sistemi kullanan cihazlar.

Önerilen Güvenlik Önlemleri

- Windows 10 v21H1, Windows 10 v20H2, Windows 10 v2004, Windows 10 v1909, Windows 10

v1903 (32 & 64 bit) işletim sistemleri kullananlar için Kasım 2021 Güncellemeleri.

- Windows 10 v1809 (32 & 64 bit) işletim sistemleri kullananlar için Mayıs 2021 Güncellemesi ile sistemlerini güncellemeleri.

İlgili İşletim Sistem ve Versiyonları

- Windows 10 v21H1 (32 & 64 bit)
- Windows 10 v20H2 (32 & 64 bit)
- Windows 10 v2004 (32 & 64 bit)
- Windows 10 v1909 (32 & 64 bit)
- Windows 10 v1903 (32 & 64 bit)
- Windows 10 v1809 (32 & 64 bit)

Referanslar

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24084
https://thehackernews.com/2021/11/unpatched-unauthorized-file-read.html
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24084
https://nvd.nist.gov/vuln/detail/CVE-2021-24084

HAVELSAN DIGITAL

Linux TIPC Modülü Zafiyeti

Regaip KURT
Siber Güvenlik Uzmanı
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

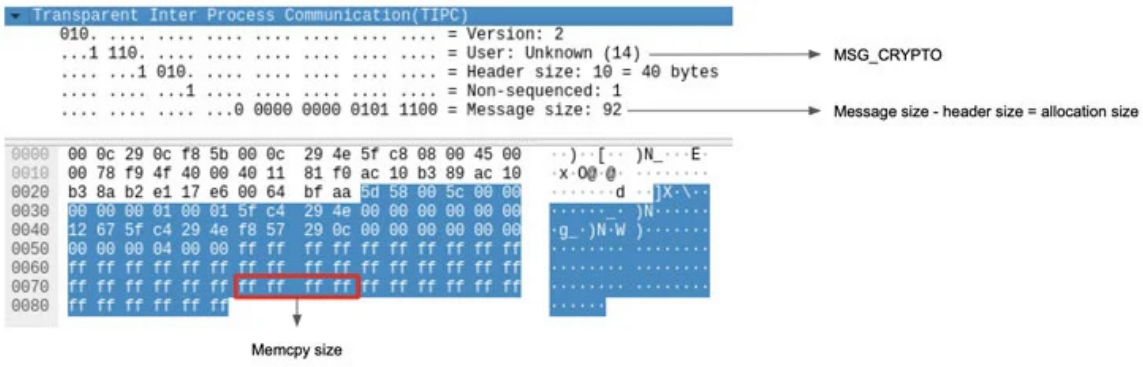
Linux TIPC Modülünde Kernel Seviyesinde Kritik Heap Overflow Zafiyeti

Zafiyet Genel Bilgi

Kasım ayının başında Linux sistemlerde ağ içi bilgisayarlar arasında iletişim kurmak için kullanılan TIPC (Transparent Inter Process Communication) modülünde herhangi bir saldırganın uzaktan kod çalıştırmasına imkan verebilen yeni bir zafiyet keşfedilmiş ve duyurulmuştur. TIPC modülü Linux sistemlerde aynı ağdaki bilgisayar kümelerinin birbirleriyle verimli bir şekilde haberleşmesini sağlamak için geliştirilmiştir. TIPC'de gecikme süreleri, bilinen diğer tüm protokollerden daha kısa ve verimliliği de TCP ile karşılaştırılabilecek seviyededir. İlgili modülün kullanılabilmesi ve çalıştırılabilmesi için sistemde etkinleştirilmiş olması gerekmektedir.

Keşfedilen zafiyet hem uzaktan hem de yerel olarak kullanılabilir ve saldırgan tarafından sömürüldüğünde kernel seviyesinde en üst düzey izinlerle sistemin ele geçirilmesi mümkün olmaktadır.

Modül içindeki tipc_crypto_key_rcv fonksiyonu diğer sistemlerden gelen anahtarları alıp iletişimde daha sonraki haberleşmenin şifresini çözmek için MSG_CRYPTO mesajlarını kullanır. MSG_CRYPTO içinde kullanıcının değiştirebileceği mesaj uzuluğun parametresinde yeterli doğrulama yapılmadan kullanılması sebebiyle Heap Overflow zafiyeti ortaya çıkmaktadır.



Yukarıdaki örnekte ağ içerisindeki bir bilgisayarın MSG_CRYPTO mesajlarını nasıl gönderdiği görülmektedir. Burada mesaj uzunluğu kısımında bellek taşırılarak saldırgana kernel seviyesinde yetkiler verilmesi mümkün olmaktadır. Böylece açıklık, ağ içinde yerel veya uzaktan bir saldırganın sistemi en üst seviyede yetkilerle ele geçirmesine imkan vermektedir.

Önerilen Güvenlik Önlemleri

TIPC modülünün etkinleştirilmediğinden emin olmak veya kernel versiyonunu 5.4.16 versiyonuna güncellemek.

Referanslar

https://nvd.nist.gov/vuln/detail/CVE-2021-43267

HAVELSAN
DIGITAL

Potensiyel Buffer Overflow, Bilgi İfşası, Siteler Arası Yazdırma

Muhammet KARAALİ
Siber Güvenlik Mühendisi
Siber Güvenlik Direktörlüğü

www.HAVELSAN.com.tr

Potensiyel Buffer Overflow, Bilgi İfşası, Siteler Arası Yazdırma

Zafiyet Genel Bilgi

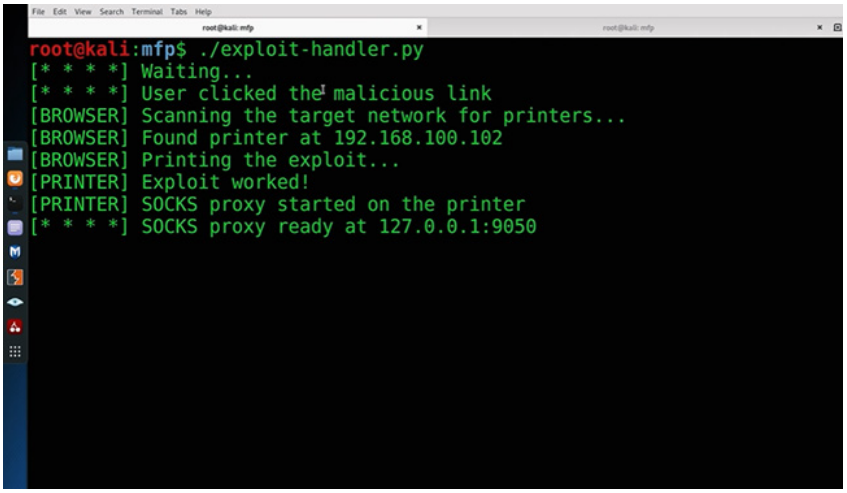
HP Yazıcılardaki güvenlik zafiyeti, Kurumsal ağların kötüye kullanılmasına olanak vermektedir; HP, 150'den fazla çok işlevli yazıcısını (MFP) etkileyen ve saldırganların savunmasız cihazların kontrolünü ele geçirmesine, bilgi çalmasına ve kurbanın ağına sızmasına olanak verebilecek önem derecesi kritik ve 9.3 olan CVE-2021-39238 potansiyel buffer over flow ve önem derecesi yüksek ve 7.1 olan CVE-2021-39237 bilgi ifşası zafiyetlerini yayınladı.

F-Secure'dan Timo Hirvonen ve Alexander Bolshev tarafından ortaya çıkarılan fiziksel erişim bağlantı noktası (port) güvenlik açığı ve yazı tipi ayrıştırma (font parsing) güvenlik açığı, görünüşe göre 2013'ten beri mevcut bulunmaktadır.

IDC'ye göre, HP'nin dünya çapındaki donanım çevre birimleri pazarının %40'ını elinde tutması nedeniyle, bu zafiyetten etkilenen yazıcılar yaygın bir şekilde bulunmaktadır. Birçok kuruluştaki güvenlik ekipleri genellikle bu cihazları, bunlarla birlikte gelen düzenli güncellemeleri yüklemek ve ağ segmentasyonunu gerçekleştirmek gibi temel güvenlik önlemlerini almayı unutmaktadır.

Zafiyetli yazıcı ağındaki güvenlik açıkları, bir saldırganın "siteler arası yazdırma" adı verilen bir saldırı başlatmasına izin verebilmektedir, ancak bu ağdaki bir kullanıcının öncelikle kötü amaçlı bir web sitesini ziyaret etmesi için kandırılması gerekmektedir.

Başarılı olursa, bu web sitesi, güvenlik açığı bulunan yazıcıda kötü amaçlarla oluşturulmuş bir yazı tipi içeren bir belgeyi uzaktan yazdırabilmektedir ve saldırgana kod yürütme hakları verebilmektedir. Aşağıda varsayımsal olarak kurbanın zararlı linke tıklaması ve bulunduğu ağdaki zafiyetli yazıcının bulunması gösterilmektedir.



Saldırgan daha sonra yazıcı aracılığıyla çalıştırılan veya önbelleğe alınan tüm bilgileri (yalnızca yazdırılan, taranan veya fakslanan belgeler değil, aynı zamanda aygıtı ağın geri kalanına bağlayan parolalar ve oturum açma kimlik bilgileri de dahil olmak üzere hepsini) fark edilmeden çalabilmektedir.

Bu arada araştırmacılar, yazı tipi ayrıştırma (font parsing) güvenlik açıklarının, etkilenen yazıcıları tehlikeye atan, ağ genelinde kendi kendine yayılan, kötü amaçlı yazılımlar oluşturmasına olanak tanıyan solucan virüslerini oluşturabileceğini belirtmektedir.

Araştırmacılar "Yetenekli bir saldırgan, beş dakikadan biraz fazla bir süre içinde fiziksel bağlantı noktalarını (portlarını) başarıyla sömürebilir. Yazı tipi ayrıştırıcısını (font parsing) kullanmak yalnızca birkaç saniye sürecektir" demektedir.

Önerilen Güvenlik Önlemleri

- CVE-2021-39238 buffer flow açığı ve CVE-2021-39237 bilgi ifşası açığı için yazıcı modelinizi https://support.hp.com/drivers'e giderek bulmanız ve yazılımını güncelleştirmeniz gerekmektedir.
- Yazıcı güvenliğinin , güvenlik duvarı ile korunan bir VLAN'da ayrı olarak tutulması gerekmektedir.
- Ayrıca, cihazlara erişimi sınırlamak, anti-tamper etiketlerini kullanmak ve yazıcıları CCTV ile izlenen alanlara yerleştirmek gibi fiziksel önlemlerin de kullanılması gerekmektedir.

Referanslar

https://portswigger.net/daily-swig/hp-printer-vulnerabilities-left-enterprise-networks-open-to-abuse-via-cross-site-printing-nbsp-attack
https://thehackernews.com/2021/11/critical-wormable-security-flaw-found.html
https://support.hp.com/us-en/document/ish_5000383-5000409-16/hpsbpi03749
https://support.hp.com/us-en/document/ish_5000124-5000148-16/hpsbpi03748

HAVELSAN
DIGITAL

Think Future

www.HAVELSAN.com.tr