STM Savunma Teknolojileri Müh. ve Tic. A.Ş.

Siber Füzyon Merkezi

Zararlı Yazılım Analiz Laboratuvarı

twitter.com/STMCyber

CVE-2019-0708 (BlueKeep) Zafiyeti İncelemesi

Hazırlayan: Mert Can Coşkuner

27 Mayıs 2019

1 Giriş

NSA araçlarının sızmasıyla birlikte MS17-010 zafiyet ve kodlarını takiben ortaya çıkan WannaCry ve Petya zararlıları pek çok kurumda hasara sebep olmuştu. Bu fidyecilik zararlılarının etkilerinin gölgesinde, Microsoft geçtiğimiz ay CVE-2019-0708 koduna ve BlueKeep ismine sahip bir güvenlik açığı için yama çıkardığını duyurdu. Güncel yama yayınlanmayan işletim sistemi versiyonları olan Windows XP ve Server 2003 versiyonlarına dahi yama yayınlanmasına sebep olan BlueKeep zafiyeti hakkında detayları, zararlı yazılım yazılıp yazılamayacağını ve zafiyeti istismar eden istismar kodu geliştirilmelerinin nasıl takip edilebileceğini aşağıda yer alan inceleme kısmında bulabilirsiniz.

2 İnceleme

14 Mayıs tarihinde Microsoft tarafından BlueKeep adıyla duyurulan CVE-2019-0708 zafiyeti; Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows XP ve Windows Server 2003 versiyonlarını etkilemektedir. ”Remote Desktop Services” hizmetinde uzaktan kod çalıştırma zafiyeti olarak tanımlanmakta ve 9.8/10 risk skoruna sahiptir.

Kullanıcının giriş yapmasına yada sistemle herhangi bir etkileşime geçmesine gerek kalmadan istismar edilebilen BlueKeep zafiyetinin, bahsettiğimiz niteliklerinden ötürü MS17-010 gibi etkilerinin olabileceği Microsoft tarafından değerlendirilmektedir.

Kritik altyapılar için yaygın kullanılan işletim sistemleri Windows 7 ve Windows 2008 R2 işletim sistemlerinin BlueKeep zafiyetinden etkileniyor olması, zafiyetin istismar kodunun geliştirilmesinin etkilerinin ne kadar büyük olabileceğini göstermektedir. Hali hazırda proof-of-concept (POC) kodları geliştirilmeye başlanmış olan BlueKeep zafiyetinin, 2019 yılı içerisinde WannaCry ya da Petya gibi geniş çaplı bir saldırıya dönüşmesi kuvvetle muhtemeldir.

3 Tavsiyeler

Eğer RDP servisini kullanmıyorsanız ve BlueKeep’in etkilediği versiyonlarda sistemlere sahipseniz, RDP servisini kapatmalısınız. Eğer RDP servisi sistemlerinizde kullanılıyorsa *”https://github.com/zerosum0x0/CVE-2019-0708”* adresinde yer alan metasploit modülü ile sistemlerinizin zafiyetli olup olmadığını kontrol edebilirsiniz. BlueKeep ile alakalı aktif olarak geliştirilen istismar kodlarından haberdar olmak için *”https://twitter.com/BlueKeepTracker”* botunu takip edebilirsiniz.

Microsoft’un *”https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708”* adresinde yayınladığı güncelleştirmenin, BlueKeep zafiyetinin etkilediği tüm sistemlerde biran önce yapılması kritik önem taşımaktadır.

Ayrıca, BlueKeep ile alakalı yayınlanan ve aşağıda yer alan suricata kuralını da sistemlerinizde kullanmanız önerilmektedir.

```
# Look for the potential signs of CVE-2019-0708, pre encryption.
#
# Note this rule is specific to port 3389, but could be expanded
# using flowbits to other ports if an earlier packet is used for
# protocol detection, or potentially a string detection on 'Duca'
# (see https://wiki.wireshark.org/RDP).
#
# Sensible values for distances between objects have been chosen.
# An exploit could potentially change the reserved byte (second
# in the packet) or pad the TPKT structure with junk to avoid the
# 'within' optimisations.
#
# 03 00                 - TPKT header: version 3, reserved byte 0
#                         Must be at the beginning of the packet
# 02 f0                 - X.224 COTP: length 2, PDU type 0x0f (DT_DATA)
```

```
# 00 05 00 14 7c 00 01 - T.124 Connect data, Generic Conference Control (ID
    0.0.20.124.0.1)
#                       PDU size ranges from 230-400 bytes, 256 skipped in
    the rule
# 03 c0                 - RDP Client Network Data
#                         Skip the header length and channel count (6 bytes)
# MS_T120 (C string)    - Name of patched control channel
#                         Must be within 372 bytes (31 channels * 12 bytes per
    channel)
alert tcp any any -> any 3389 (msg:"NCC GROUP RDP connection setup with
    MS_T120 channel, potential CVE-2019-0708"; flow:to_server,established;
    content:"|03 00|"; offset:0; depth:2; content:"|02 f0|"; distance:2; within
    :2; content:"|00 05 00 14 7c 00 01|"; within:512; content:"|03 c0|";
    distance:3; within:384; content:"MS_T120|00|"; distance:6; within:372;
    threshold: type limit, track by_src, count 2, seconds 600; classtype:bad-
    unknown; reference:url,portal.msrc.microsoft.com/en-US/security-guidance/
    advisory/CVE-2019-0708; sid:1; rev:1;)
```