Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability

written by Mert SARICA | 20 Kasım, 2009

15 Ocak 2009 tarihinde gerçekleştirdiğim penetrasyon testinde Juniper SSL VPN cihazında keşfettiğim bir güvenlik zafiyetinin detaylarına girmeden ufak bir bölümünü 16 Temmuz 2009 tarihinde netsec grubunda paylaşmıştım, üretici tarafından düzeltildiği için artık Juniper SIRT ile yaptığım bir kaç yazışmayı ve zafiyetin içeriğini sizlerle paylaşabilirim.

_____
From: Payum Moussavi
Sent: Thursday, July 16, 2009 6:48 PM
Subject: RE: Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability…

Hello Mert,

This issue is fixed in the following releases:

6.4R2 and Higher – Released
6.3R5 – Released
6.2R6 – Released
6.1R8 – Sept/09 – no date confirmed.

Download URL for IVE software:
http://www.juniper.net/techpubs/software/ive/

Our Advisory will be coming out at the end of Sept early October.

Regards,
Payum Moussavi

_____

Kimden: Payum Moussavi
Gönderilmiş: Per 19.02.2009 20:27
Konu: RE: Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability…
Hello Mert,

Our risk assessment for this issue is “Low”. In order to exploit this vulnerability you would need physical access or remote access (exploiting another vulnerability) to the machine.

As stated, we will fix this issue in Q3/09.

Regards,
Payum Moussavi

SLT Escalation Team, Manager
Juniper Technical Assistance Center (JTAC)

Service Layer Technology (SLT) Group
Juniper Networks, Inc.

_____

——Original Message——
From: MERT SARICA
Sent: Monday, January 26, 2009 5:32 AM
Subject: RE: Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability…

…
First of all consider that our default policy (dsjvd.ini) has a configuration line as
AllowedApps=iexplore.exe^firefox.exe^mstsc.exe^dshostchecker.exe^dsCacheCleaner.exe^dsNCService.exe^dsNetworkConnect.exe^dsAccessService.exe^getflash.dll^msi.dll^telnet.exe

Attack steps:

1- I set a custom dsjvd.ini with AllowedApps=* and put it into C:\Documents and Settings\Administrator\Application Data\Juniper Networks\Host Checker\policy_1\ folder.
2- I opened up C:\Documents and Settings\Administrator\Application Data\Juniper Networks\Host Checker\policy_1\dsjvd.ini and put it into background, made it ready for save attempt in the 4th step.
2- I fired up the web browser and called https://****/Profile
3- Web server redirected me to https://***/dana-na/auth/url_9/welcome.cgi
4- While it was loading the components and secure workspace, I brought previously opened dsjvd.ini to the front and tried a save attempt frequently like 20 save attempts in 5 seconds.
5- As a result, TOC/TOU vulnerability occured, my custom policy loaded into the workspace and I was able to run any process like nmap in the screenshot sample as I sent to you before.

I hope steps are clear enough.