Sårbarheter i routrar och switchar

SARA DANNERUD

KTH Information and Communication Technology

Bachelor of Science Thesis
Stockholm, Sweden 2008

COS/CCS 2008-03

Sårbarheter i routrar och switchar

Sara Dannerud

3 Mars 2008

Handledare: Carl-Johan Bostorp, High Performance Systems
Examinator: Professor Gerald Q. Maguire Jr., KTH

Sammanfattning

Det finns många olika källor där man kan få information om sårbarheter i routrar och switchar. Mängden information gör det dock svårt att på ett enkelt sätt ta reda på vilka tillverkare som drabbas och vilken typ av sårbarheter man hittar i nätverksutrustning. Därmed är det också svårt att veta hur man ska skydda sin utrustning mot attacker.

I detta examensarbete analyseras ett antal befintliga sårbarheter i routrar och switchar. Dessa sårbarheter har valts ut genom att i National Vulnerability Database söka på orden ”router” och ”switch”. Målet med analysen är att svara på frågorna vem, vad och varför när det gäller sårbarheter i routrar och switchar.

Examensarbetet beskriver vilka tillverkare som drabbas av sårbarheter, vilka typer av sårbarheter som är vanligast i routrar och switchar och varför sårbarheterna har uppstått. Utifrån detta dras slutsatser om vad man som användare ska göra för att undvika attacker mot sin utrustning. I arbetet beskrivs också hur tillverkarna väljer att hantera de sårbarheter som finns i deras produkter.

Abstract

There are a lot of different sources to information about vulnerabilities in routers and switches. The amount of information means that there is no easy way to find out which vendors are affected by vulnerabilities and what types of vulnerabilities that are found in network equipment. Thereby it is also hard to know how to protect your equipment against attacks.

In this thesis a number of already existing vulnerabilities in router and switches are being analyzed. These vulnerabilities have been chosen by searching the National Vulnerability Database using the words “router” and “switch”. The aim of the analysis is to answer the questions who, what and why when it comes to vulnerabilities in routers and switches.

The thesis describes which vendors are exposed to vulnerabilities, what types of vulnerabilities that are most common among routers and switches and why these vulnerabilities have came up. Based on this information, conclusions are drawn regarding what the user should do to avoid vulnerabilities in their equipment. The way the companies deal with vulnerabilities in their products is also described.

Innehållsförteckning

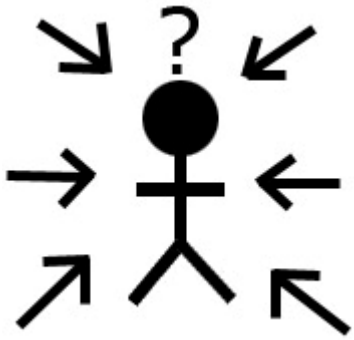
1 Problembeskrivning

1.1 Bakgrund

Sårbarheter i routrar och switchar är ett område som inte är speciellt väl utforskat. Söker man på nätet så hittar man mycket information men mängden information innebär också att det är tidskrävande att ta fram en samlad bild över vilken typ av hot och sårbarheter som finns. Detta är också ett område som omges av fördomar. Systemadministratörer sätter ofta fokus på säkerheten i systemets servrar och databaser men bryr sig ibland inte ens om att uppdatera mjukvaran i sin router så länge allt fungerar som det ska [48]. Anledningen till detta kan dels vara att man lever i tron att routrar och switchar inte utsätts för angrepp och dels att man saknar kunskap om var sårbarheterna finns och därmed var man ska sätta in sina resurser. Problemet är att om någon lyckas ta över dina routrar eller switchar så har han snart kontroll över hela nätverket vilket självklart kan få allvarliga konsekvenser.

1.2 Mål

Målet med examensarbetet är att ta fram ett underlag för att kunna bedöma hur, var och under vilka omständigheter angrepp mot routrar och switchar förväntas dyka upp. Det finns idag ett antal källor där man kan få information om sårbarheter, bland annat databaser, mailinglistor och olika webbsidor. Problemet är att det tar tid att få fram och sammanställa information från alla dessa källor. Syftet med denna rapport är därför att ta fram en samlad bild över vilka sårbarheter som förekommer och vilka tillverkare som drabbas. Målgruppen för arbetet är främst nätverksarkitekter på företag men även andra personer som hanterar nätverksutrustning, privat eller i jobbet, kan ha intresse av att läsa rapporten. Genom att ge dessa personer en överblick över vad de ska tänka på när det gäller säkerheten relaterad till deras utrustning kan de spara tid. Rapporten ska både rikta in sig på sårbarheter hos specifika tillverkare men även ta upp mer generella problem som drabbar många olika tillverkare. Med kunskap om detta ska man sedan kunna minimera riskerna och lättare bedöma var resurserna ska läggas när det gäller att upptäcka och förhindra intrång.



Figur 1:1 Många källor till information

Genom arbetet ska följande frågor få ett svar:

- Vilken typ av utrustning och vilka tillverkare är det som drabbas?
- Vad är orsaken till att sårbarheterna uppstått och vad krävs för att utnyttja dem?
- Vilken typ av sårbarheter handlar det om; hur tekniskt avancerade är det och vad händer om de utnyttjas?
- Hur många sårbarheter hittar man per år och hur ser utvecklingen ut över tiden?
- Var dyker dessa sårbarheter oftast upp, är det till exempel något specifikt protokoll eller någon speciell mjukvara som ofta drabbas?
- Kan man eventuellt urskilja någon händelse med stark påverkan?

1.3 Metod

Common Vulnerabilities and Exposures (CVE) [1], är en lista över publikt kända sårbarheter i datasystem. CVEs funktion är att ge kända sårbarheter ett allmänt namn, en identifierare, och en standardbeskrivning vilket gör att sårbarheten blir lätt att hitta och lätt att jämföra med andra sårbarheter. Detta var tidigare ett problem då olika databaser använde olika namn och beskrivningar på sårbarheterna. Sårbarheterna i CVE har en status som är antingen ”entry” eller ”candidate” beroende på om de ingår i listan eller fortfarande väntar på att bli accepterade.

Med hjälp av National Vulnerability Database (NVD) [2], kan man söka på alla sårbarheter som är listade i CVE och det är denna databas som ska användas som underlag för datainsamlandet i detta arbete. Genom att söka på orden ”router” och ”switch” i NVD med kriteriet att sårbarheten inte får vara äldre än år 2000 ska relevant data tas fram. Årtalet 2000 är valt dels med tanke på att CVE skapades först 1999 [11] och dels med tanke på att inte tidsspannet skulle bli för stort. Att avgränsa sökandet från år 2000 och framåt kommer troligen att innebära att några produkter kommer att se ut att ha drabbats av färre sårbarheter än vad de faktiskt har. Denna rapports syfte är dock att ge en generell bild över tillverkare, produkter och sårbarheter, inte att detaljstudera specifika fall, så därför får detta anses ha en mindre betydelse. För varje träff i NVD listas ett antal värden och information om sårbarheten ordnade under ett antal rubriker. Från detta ska viss information väljas ut och sparas i kalkylblad som skapas i Microsofts program Excel för att sedan kunna användas som underlag för analysen.

Den information som jag bedömer nödvändig att spara ned från NVD för att kunna svara på frågorna i målformuleringen är “CVE Identifier number”, “Original release date”, “Overview”, “CVSS v2 Base score “, “Access Vector”, “Access Complexity”, “Authentication”, “Impact Type”, “Vulnerable software and versions” och “Vulnerability Type”.

1.4 Omfattning och avgränsningar

Undersökningen och analysen kommer endast att baseras på de relevanta resultat som listas när man söker på ”router” och ”switch” från år 2000 och framåt i NVDs databas. För tydlighetens skull bör det påpekas att en sökning på orden ”router” och ”switch” sannolikt kommer att innebära att ett antal sårbarheter aldrig påträffas, trots att det rör sårbarheter i just denna typ av utrustning. Anledning är i så fall att orden ”router” eller ”switch” inte förekommer i informationen om sårbarheten.

För varje enskild sökträff kommer endast ovan nämnda parametrar att dokumenteras. All övrig information som kommer upp i samband med visning av en sårbarhet kommer ej att antecknas då den inte utgör någon grund för att kunna besvara de frågor som ställs i målformuleringen. Hänsyn kommer ej heller att tas till de CVE identifierare som ännu inte har fått entry status. Fokus i analysen kommer att ligga på stora tillverkare och/eller sårbarheter som förekommer vid upprepade tillfällen då de skulle bli allt för tidskrävande att analysera varenda tillverkare, deras produkter och tillhörande sårbarheter som har förekommit i NVD sedan år 2000.

2 Teori

2.1 Sårbarhet

En sårbarhet kan beskrivas som en svaghet i ett system vilken kan utnyttjas för att ta sig in i och utföra handlingar som kan skada eller påverka systemet. Orsaken till att sårbarheten uppstår kan till exempel vara en bugg i en programvara eller ett designfel [5].

2.2 Denial of Service

Denial of Service (DoS) är en typ av attack vars syfte är att få ett system att sluta fungera som det ska vilket leder till att användare inte längre kommer åt dess tjänster och resurser. Det finns ett antal huvudtyper av DoS-attacker [6][7]:

- Konsumtion av resurser, som bandbredd (vilket är det vanligast förekommande), CPU-tid eller hårddiskutrymme.
- Förändra konfigureringsinformation, till exempel information om routes och DNS.
- Orsaka störningar i nätverkskommunikationen mellan server och klient.

När det gäller routrar och switchar är det vanligt med attacker som innebär att resurser konsumeras, till exempel genom flood-attacker. En flood-attack är en typ av DoS-attack som går ut på att skicka en överväldigande mängd datapaket till ett system. Det är också vanligt att en attack orsakar störning i kommunikationen genom att utrustningen går ner eller startar om, vilket ofta blir konsekvensen vid till exempel felaktigt utformade datapaket.

2.3 Spoofing

Spoofing innebär att uppge en falsk identitet i syfte att komma åt information som man annars inte skulle ha tillgång till. Exempel på detta kan vara att skicka iväg ett mail under falskt namn eller att använda sig av en falsk IP-adress.

2.4 Problem relaterade till specifika protokoll

Hos routrar och switchar förekommer det en del sårbarheter som är relaterade till olika dataprotokoll. Angriparen utnyttjar de standarder/regler som finns i protokollen på ett felaktigt sätt, till exempel genom att ändra i ett datapaket, vilket får olika typer av konsekvenser.

2.4.1 ICMP

Internet Control Message Protocol (ICMP) är det protokoll som ansvarar för att skicka felmeddelanden mellan enheter i nätverket. Verktyget ping använder sig av ICMPs ”Echo request" och "Echo reply” för att verifiera att en maskin är nåbar.

Ett förekommande problem bland routrar och switchar är en DoS-attack som kallas för ”Ping of death”. Attacken går ut på att skicka ICMP-paket med större storlek än vad som är tillåtet vilket inte mottagarsystemet kan hantera. Ett IP-paket får enligt standard inte vara större än

65,536 bytes [43]. Angriparen utnyttjar att stora paket delas upp i mindre delar, fragment, innan det skickas till mottagaren. Genom att i det sista fragmentet skicka med mer data än vad som är tillåtet kommer den totala tillåtna storleken på 65,536 bytes att överskridas när fragmenten sätts ihop till ett paket igen hos mottagaren. Detta resulterar ofta i en systemkrasch. Problemet är egentligen inte direkt relaterat till ICMP utan samma attack kan utföras med andra typer av IP-paket. Det ska dock nämnas att denna sårbarhet är ovanlig nuförtiden då de flesta system nu är patchade för att undvika denna typ av attack [44].

En annan typ av attack är ping-flooding där angriparen skickar en stor mängd ”Echo request” till offret som svarar med ”Echo reply”. Angriparen hoppas att offret inte ska klara av att hantera all trafik vilket då leder till DoS. En förutsättning för att denna attack ska lyckas är dock att angriparen har bättre bandbredd än offret då denna attack är resurskrävande för båda parter.

2.4.2 TCP

Transmission Control Protocol (TCP) är det protokoll som används för tillförlitlig dataöverföring. Ett problem relaterat till TCP är SYN-flood. För att en TCP-anslutning ska etableras måste klient och server utbyta en sekvens av meddelanden. Klienten skickar först ett SYN-medddelande till servern. Serverns svarar då med att skicka ett SYN-ACK tillbaka till klienten som i sin tur svarar med ett ACK-meddelande till servern. Därefter är anslutningen etablerad. Detta kallas för ett ”three-way handshake”. Vid en SYN-flood attack utnyttjar angriparen detta tillvägagångssätt genom att skicka iväg en stor mängd SYN-meddelanden med en felaktig avsändaradress till servern. Servern skickar då tillbaka SYN-ACK-meddelanden till denna felaktiga adress och förväntar sig därefter ett ACK-meddelande som svar. Detta sista ACK-meddelande kommer dock aldrig att dyka upp vilket skapar en halvöppen anslutning där servern har allokerat resurser för den anslutning som den tror ska etableras. Om detta händer tillräckligt många gånger kommer serverns resurser till sist ta slut vilket leder till DoS.

Ett annat problem är förutsägbara TCP Initial Sequence Numbers (ISN). Angriparen kan ta över en redan existerande TCP-session genom att utge sig för att vara en av deltagarna i sessionen. Detta sker genom att angriparen skickar ett paket till måldatorn med samma sekvensnummer och käll-IP-adress som den riktiga avsändaren. Detta paket måste dessutom anlända före paketet från den riktiga avsändaren.

2.4.3 UDP

User Datagram Protocol (UDP) används vid förbindelselös dataöverföring. Även UDP kan användas för att utföra en flood-attack. Angriparen skickar ett UDP-paket till en slummässigt vald port på måldatorn. Måldatorn kommer då att se efter vilken applikation som finns på denna port och, när den inser att det inte finns någon applikation, svara med ett ”ICMP destination unreachble”. Görs detta tillräckligt många gånger inträffar en DoS då systemet går ner.

En vanlig portscanning kan även den ha effekten att systemet går ner om det påverkas för mycket av scanningen. Detta gäller oavsett vilket protokoll som används

2.4.4 HTTP och administrationsgränssnitt

Många tillverkare ger användaren möjligheten att genom ett administrationsgränssnitt konfigurera en router eller switch via webben. Denna tjänst kan vara påslagen som standard, trots att användaren kanske inte använder tjänsten. En angripare kan via detta gränssnitt använda sig av olika typer av HTTP-requests för att utföra en attack, något som ofta resulterar i DoS men ibland också i att angriparen kan ta del av känslig information.

2.4.5 SNMP

Simple network management protocol (SNMP) är ett protokoll som används för nätövervakning och som ibland förekommer i samband med sårbarheter i routrar. Sårbarheterna uppstår ofta i samband med standardinställningar för SNMP ”community string”. Ett problem är att SNMP ofta är påslaget automatiskt utan användarens kännedom [39] vilket ökar risken

2.5 Lösenordshantering i nätverksutrustning

Många tillverkare använder sig av standardinställningar för användarnamn och lösenord på de produkter som levereras till kunder. Bland annat gäller detta de flesta av de routers som är populära bland hemanvändare [49]. Problemet är att många användare sedan inte bryr sig om att ändra dessa inställningar. När det gäller trådlös utrustning för hemanvändare är det ungefär 50 % som inte bryr sig om att ändra detta [32]. Anledningen kan vara att användarna inte inser faran med att behålla standardinställningarna, och därför inte bryr sig, eller att de faktiskt inte vet att deras utrustning har ett lösenord överhuvudtaget. För en angripare som vill utnyttja detta är det inga problem att ta reda på de standardinställningar som tillverkarna använder då det finns ett antal sidor som enbart riktar in sig på information om detta, till exempel Default Router Password Database [26]. Cisco och Linksys har på senare tid, enligt egna uppgifter, blivit bättre på att hantera detta problem [27]. Lösningen är att vid installation ge användaren anvisningar för att ändra det standarinställda lösenordet. Användaren kan dock välja att hoppa över detta utan att det på något vis påverkar routerns funktion. Även Netgear har på sin hemsida information om att man bör ändra standarinställningar för lösenordet [33]. Företagen verkar dock inte vara speciellt intresserade av att ta fram en lösning som tvingar användaren att ändra sitt lösenord. Enligt Michael Scott, teknisk chef på D-Link, skulle en sådan lösning resultera i att kunderna returnerade sina produkter och valde en produkt från ett konkurrerande företag [27].

För att minimera risken för att obehöriga tar sig in i ett system med hjälp av standardinställningar för lösenord och användarnamn så bör ett företag alltid ha någon typ av säkerhetspolicy där man specificerar hur hanteringen av lösenord ska skötas. På detta vis minskar man risken för att obehöriga kan ta sig in i systemet.

2.6 Datainsamlingen

2.6.1 Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE), skapades 1999 och är en lista över publikt kända sårbarheter, så kallade CVE Identifiers. Syftet med CVE är att ge såbarheterna ett allmänt namn, en identifierare, och en standardiserad beskrivning för att på så vis underlätta när informationen om sårbarheten till exempel ska delas mellan databaser eller användas i

något verktyg. Figur 2:1 visar ett exempel på hur en CVE Identifier kan se ut. Varje CVE Identifier består av:

- Ett identifikationsnummer. (1)
- En kort beskrivning av sårbarheten. (2)
- Status som kan vara antingen ”entry” eller ”candidate”. (3)
- Relevanta referenser. Till exempel till en rapport om sårbarheten. (4)

Name: CVE-2001-0751 (1)
Description:
Cisco switches and routers running CBOS 2.3.8 and earlier use predictable TCP Initial Sequence Numbers (ISN), which allows remote attackers to spoof or hijack TCP connections. (2)
Status: Entry (3)
Reference: CISCO:20010522 More Multiple Vulnerabilities in CBOS (4)
Reference: URL:http://www.cisco.com/warp/public/707/CBOS-multiple2-pub.html (4)
Reference: XF:tcp-seq-predict(139) (4)
Reference: URL:http://xforce.iss.net/static/139.php (4)

Figur 2:1 Exempel på en CVE Identifier

Organisationen MITRE, som står bakom CVE, får information om sårbarheterna i första hand från organisationerna Internet Security Systems (ISS), SecurityFocus, Neohapsis och U.S. National Infrastructure Protection Center. Varje ny sårbarhet som upptäcks tilldelas ett CVE nummer och får candidate status. Candidate status ges till en nyligen upptäckt sårbarhet som ska tas upp till diskussion av CVE Editorial Board. CVE Editorial Board består av ett antal representanter för säkerhetsrelaterade företag och organisationer och dessa personer röstar om huruvida en kandidat ska accepteras eller inte. Om CVE Editorial Board beslutar sig för att acceptera sårbarheten får den entry status vilket innebär att den får vara med i CVEs lista över sårbarheter. Om en kandidat inte blir accepterad kan det bero på att sårbarheten är alltför lik en tidigare kandidat eller att det vid ytterligare efterforskningar visar sig att sårbarheten inte existerar.

2.6.2 Begränsningar i CVE

En del av de sårbarheter som har candidate status har haft det väldigt länge, vissa sedan många år tillbaka. Anledningen är att de inte får tillräckligt många positiva röster för att kunna tas med i listan. Detta kan innebära att en sårbarhet aldrig blir accepterad och kan tas med i listan trots att det kanske handlar om en sårbarhet som egentligen borde finnas där. Ännu finns inget svar på hur problemet med dessa ”permanenta” kandidater ska lösas [50].

Man bör också fundera över vilka sårbarheter som förekommer i CVE överhuvudtaget. De organisationer som rapporterar in sårbarheter till CVE baserar sin information på erfarenheter från produkter som de själva använder alternativt hämtar de information från olika källor som de kommer i kontakt med. Detta kommer självklart att återspegla sig i vilka sårbarheter som presenteras i CVE. Med andra ord är informationen inte heltäckande och många sårbarheter kommer aldrig att dyka upp i CVE trots att de är välkända.

Man kan också jämföra sannolikheten för att en sårbarhet riktad mot företagsutrustning hamnar i CVE jämfört med en sårbarhet riktad mot utrustning för hemanvändare. Den utrustning som riktar sig mot hemanvändare och mindre företag hanteras, antagligen, i stor utsträckning av människor med små och ofta begränsade kunskaper om hur utrustningen fungerar. Av detta kan man dels dra slutsatsen att det är en mindre chans att de upptäcker en sårbarhet överhuvudtaget och även om de skulle göra det så är gissningen att de i mindre utsträckning skulle bry sig om att rapportera sårbarheten till någon. Detta kan jämföras med de människor som till exempel jobbar med nätverksutrustningen på ett större företag, eller de personer som finns bakom de organisationer som rapporterar till CVE. Dels har de, med största sannolikhet, en mycket större kunskap inom området jämfört med en vanlig användare vilket gör att de lättare upptäcker felen. Förmodligen har de även ett intresse för säkerheten i nätverket vilket gör att de håller sig uppdaterade genom till exempel nyhetsbrev och forum. Detta innebär att de vet hur det ska bära sig åt för att informera om sårbarheten och att de även inser vikten av att informera det drabbade företaget och andra användare om sårbarheten i fråga. Man kan av detta dra slutsatsen att de sårbarheter som drabbar utrustning hos stora företag i större mån återfinns i CVE än de sårbarheter som drabbar utrustning riktad mot hemanvändare och små företag. Man ska dock inte bortse från att de personer som dagligen arbetar med nätverksutrustning sannolikt även använder sig av routrar och switchar privat vilket gör att även produkter för hemanvändare blir granskade på ett ”professionellt” sätt.

2.6.3 National Vulnerability Database

National Vulnerability Database (NVD) är en databas där man kan söka på de sårbarheter som listas i CVE. I NVD får man, utöver den information som finns i CVEs lista, även information om vilken hård- och mjukvara sårbarheten gäller samt länkar till externa källor med mer information och buggifxar. Sårbarheten är också poängsatt och bedömd enligt Common Vunerability Scoring System (CVSS) [3].

2.6.4 Common Vulnerability Scoring System

CVSS är en modell som används för att kunna bedöma sårbarheter och ge dem en sammansatt poäng som får representera hur allvarlig sårbarheten är och vilken risk den innebär. CVSS använder sig av sex olika basvektorer för att bedöma sårbarheten:

Access Vector
Beskriver vilken typ av åtkomst som krävs till det system där sårbarheten finns. Lokal åtkomst innebär att man måste ha fysisk access till systemet eller ett lokalt konto för att utnyttja sårbarheten medan nätverksåtkomst innebär det rakt motsatta, att sårbarheten kan utnyttjas utan lokal åtkomst.

Access Complexity
Handlar om hur komplicerat det är att utnyttja sårbarheten. Utöver att få åtkomst till systemet kan det krävs ytterligare steg för att utnyttja sårbarheten. Värdena är hög, medium och låg där låg bland annat innebär att det endast krävs lite kunskaper för att utnyttja sårbarheten och att produkten det handlar om ofta är inställd på en standardkonfigurering. Ett högt värde kan handla om en sårbarhet som inte förekommer så ofta i praktiken eller där det krävs att den som utnyttjar sårbarheten redan har utökade rättigheter.

Authentication
Talar om hur många gånger en angripare måste identifiera sig, t.ex. logga in på ett operativsystem, för att kunna utnyttja sårbarheten.

Confidentiality Impact
Handlar om i vilken mån en angripare kommer åt skyddad information på det angripna systemet.

Integrity Impact
Integritet handlar i det här fallet om att kunna lita på att den information som finns är riktig. Om en angripare kan gå in och ändra i valfri fil på det angripna systemet så äventyras integriteten helt.

Availability Impact
Tillgänglighet handlar om vilken påverkan ett lyckat angrepp har på systemet. Då ett angrepp till exempel kan kräva mycket bandbredd, hårddiskutrymme eller processorkraft kan det innebära begränsad tillgänglighet till resurser i systemet eller i värsta fall att hela systemet går ner.

Faktorerna ovan utgör underlag för de beräkningar som utförs och som slutligen leder fram till CVSS Base Score. Poängen har ett värde mellan 1-10 där 0.0-3.9 är låg allvarlighet, 4.0-6.9 är medel allvarlighet och 7.0-10.0 är hög allvarlighet [4].

3 Metod

3.1 Arbetets genomförande

Det första skedet i datainsamlingen var att i National Vulnerability Database söka på orden router och switch med kriteriet att sårbarheten inte får vara äldre än år 2000. Detta resulterade totalt i ungefär 400 träffar. Av dessa träffar finns dock ett antal som kan sorteras bort då det antingen inte har något med sårbarheter i routrar och switchar att göra eller ännu inte har fått entry status. För varje relevant träff ska följande data dokumenteras i Excelfilen:

CVE Identifier number
Original release date
Overview
CVSS v2 Base score
Access Vector
Access Complexity
Authentication
Impact Type
Vulnerable software and versions
Vulnerability Type

I Excelfilen ska vissa av dessa data sorteras upp ytterligare för att lättare kunna analyseras. “Vulnerable software and versions” delas upp i tillverkare och mjukvara och ”Original release date” delas upp i år och månad. Dessutom tillkommer kolumner där relevanta data från översiktstexten plockas ut, detta för att lätt kunna skilja ut denna information från övrig text. Det kan till exempel vara information om vilken typ av attack som har använts eller om det är något speciellt protokoll som har utnyttjats. Eftersom all data sparas i Excelfiler blir det sedan lätt att, med hjälp av programmets filter- och sorteringsfunktioner, ta fram det data som behövs vid besvarandet av varje specifik frågeställning. Jag har även i vissa fall använt mig av databasen hos SecurityFocus [12] för att hämta ut information. Denna databas klassificerar, när det är möjligt, sårbarheterna utifrån orsaken till att de har uppstått, till exempel ”Design Error” eller ”Access Validation Error”. Då jag inte kunde hitta någon liknande information i NVD, och då jag anser att detta kan vara användbart vid analysen av datat, har även denna information adderats till Excelfilerna.

Vid analysen av datat kommer resultaten, där det är möjligt och relevant, att presenteras uppdelade efter respektive tillverkare. Detta för att man lätt ska kunna ta del av resultaten för den tillverkare man främst är intresserad av.

4 Analys

4.1 Drabbade tillverkare och utrustning

I det insamlade datat återfinns 256 stycken olika sårbarheter. Av dessa är 183 stycken sårbarheter som har hittats i routrar och 73 stycken sårbarheter som har hittats i switchar. Sårbarheterna i routrarna är fördelade på 57 stycken olika tillverkare och sårbarheterna i switcharna på 19 olika tillverkare. Majoriteten av tillverkarna förekommer bara med en eller två sårbarheter.

Tittar man på resultaten så ser man att det företag som inte har så många träffar ofta är mindre företag med små marknadsandelar. Ett litet företag med små marknadsandelar har ett färre antal personer som använder deras produkter och följaktligen är chansen att någon upptäcker en sårbarhet mindre. På samma sätt har ett marknadsledande företag en stor kundkrets och därmed är chansen större att en sårbarhet upptäcks. En person som aktivt letar efter sårbarheter att utnyttja får också en större ”utdelning” om han eller hon hittar en sårbarhet i utrustning tillverkad av en stor tillverkare eftersom det då finns många mål att angripa.

4.1.1 Sårbarheter i routrar

I Tabell 4:1 visas de femton tillverkare som vid en sökning på ordet router i NVD förekommer med 3 eller flera sårbarheter. De tillverkare som bara förekommer en eller två gånger är inte listade i tabellen. Dessa 15 tillverkare i tabellen nedan står tillsammans för 126 stycken av de 183 sårbarheter som hittades vid en sökning på ordet router. Detta innebär att 26 % av tillverkarna står för nästan 70 % av de funna sårbarheterna.

Tittar man närmare på tabellen så ser man att de 3 tillverkare som har flest antal funna sårbarheter tillsammans står för 50 % av alla sårbarheter i denna grupp. Utvidgar man detta till de 6 värst drabbade tillverkarna så står dessa för ungefär 70 % av alla sårbarheter hos de tillverkare som har drabbats av sårbarheter tre gånger eller fler.

Som framgår av tabellen så är det inte helt oväntat hos Ciscos routrar som flest sårbarheter återfinns då Cisco länge har varit marknadsledande inom området [15] och för närvarande har en marknadsandel på ungefär 60 % [46]. I gruppen som presenteras ovan står Cisco för ungefär 28 % av sårbarheterna. Tittar man istället på alla 183 sårbarheter hos routrarna så återfinns 20 % av dessa i en Ciscoprodukt.

Högt upp i tabellen placerar sig också LinkSys (som ägs av Cisco), NetGear och D-Link, även de kända aktörer på marknaden. En skillnad mellan dessa 3 företag och Cisco är att LinkSys, NetGear och D-Link i första hand riktar sig mot mindre företag och hemanvändare [17][18][19] medan de produkter som tillverkas under varumärket Cisco främst används av större företag och operatörer [16].

Tabell 4:1 Routers, antal sårbarheter per tillverkare med över 3 träffar

Tillverkare	Antal sårbarheter på sökord ”router”	Antal sårbarheter, %	Kumulativ, %
Cisco	35	27,78	27,78
LinkSys	16	12,70	40,48
NetGear	12	9,52	50,00
D-Link	9	7,14	57,14
ZyXEL	9	7,14	64,28
3Com	8	6,35	70,63
Belkin	7	5,56	76,19
Nortel	5	3,97	80,16
Cayman	4	3,17	83,33
Edimax	4	3,17	86,50
Mentor	4	3,17	89,67
SMC Networks	4	3,17	92,84
2Wire	3	2,38	95,22
Netopia	3	2,38	97,6
Siemens	3	2,38	99,98

På marknaden som riktar sig mot större företag och operatörer är Juniper det företag som har den näst största marknadsandelen efter Cisco [9][10]. När det gäller core-routers är Cisco och Juniper de två företag som är dominerande med 61 % respektive 35 % av marknaden [38]. Trots detta finns inte Juniper med i tabellen ovan. Anledningen till detta är att det bara finns 2 sårbarheter hos Junipers produkter registrerade i NVD. Vid ytterligare sökningar i NVD på enbart sökordet ”juniper” så visar det sig att det finns tre sårbarheter till som rör Junipers routrar. Dessa sårbarheter gäller JUNOS, det operativsystem som körs på alla Junipers routerserier. Anledningen till att dessa tre resultat inte dök upp vid den första sökningen är att ordet ”router” inte förekommer i informationen om dessa sårbarheter. En sökning på Google med orden ”juniper”, ”vulnerabilities” och ”router” ger inga andra resultat än de sårbarheter som redan finns listade i NVD. Det verkar alltså, om man ser till dessa resultat, som att det faktiskt inte förekommer så mycket sårbarheter hos Junipers routrar. Dock kan nämnas att de två sårbarheter som dök upp vid den ursprungliga sökningen har en CVSS Base Score på 7.5 respektive 10.0 vilket alltså handlar om allvarliga sårbarheter.

Olika typer av utrustning används på olika sätt i nätverken och den effekt som en attack har beror på vilken typ utrustning som angrips. En attack mot en core-router kan ha en enormt stor påverkan på trafiken i ett nätverk medan en attack mot en router som står hemma hos en privatperson bara drabbar just detta hushåll. Detta kan vara en bidragande orsak till att det inte finns så många sårbarheter rapporterade hos Juniper. Man kan misstänka att företag som använder sig av denna typ av utrustning med avsikt väljer att ligga lågt och inte informera vare sig om att de äger utrustningen eller eventuella problem som uppstår. Detta på grund av att konsekvenserna vid en attack skulle bli så omfattande. Tittar man på Ciscos core-router, CRS-1, så har även den bara ett fåtal träffar i NVD.

4.1.2 Sårbarheter i switchar

Även inom switchar är Cisco den största tillverkaren [13] med en marknadsandel på ungefär 70 % [46] och precis som när det gäller routrar så toppar de statistiken över funna sårbarheter vilket man kan se i Tabell 4:2. Hos Ciscos switchar har 40 sårbarheter hittats vilket innebär att

de står för ungefär 55 % av alla sårbarheter hos switcharna. Värt att notera i tabellen är det stora glappet som finns mellan Cisco och nästa tillverkare på listan, HP. HP är näst störst på switchmarknaden [13] och har en global marknadsandel på ungefär 17 % [14]. Trots detta finns bara 4 träffar i NVD. Vid en sökning i OSVDB [8] på ”switch” och ”HP” blir det inga träffar alls och hos SecurityFocus [12] hittar man samma sårbarheter som i NVD. En sökning på Google ger också ett liknande resultat. De första träffarna på ”vulnerabilities” ”HP” och ”switch” är alla sådana som återfinns i NVD.

Tabell 4:2 Switchar, antal sårbarheter per tillverkare

Tillverkare	Antal sårbarheter på sökord switch
Cisco	40
HP	4
3Com	3
Allied Telesis	3
Alcatel	2
Asante	2
Brocade	2
Foundry Networks	2
Intel	2
Marconi	2
Nortel	2

HP erbjuder sina kunder livstids garanti på ProCurve-serien [40], vilket är den produktserie som switcharna tillhör. Detta skulle kunna vara en anledning till det låga antalet sårbarheter då garantin innebär att HP måste arbeta kontinuerligt med produkterna och hanteringen av de problem och sårbarheter som uppstår.

4.1.3 Cisco

Sårbarheterna i Ciscos sortiment är spridda över många produkter och både hård- och mjukvara är drabbade. Majoriteten av de sårbarheter som förekommer i Ciscos produkter är mer än tre år gamla och därav återfinns många av sårbarheterna hos produkter som inte längre tillverkas. Detta innebär dock inte att det inte längre finns någon som använder dessa produkter, faktum är att de fortfarande kan ha ett stort antal användare. De produkter bland routrarna där de ett flertal gånger har förekommit sårbarheter är 12000-serien, 600-serien och SN5420. Varken 600-serien och SN5420 tillverkas längre [21][22]. Bland switcharna är olika modeller i Catalyst-serierna drabbade ett antal gånger. Många fel återfinns också hos Ciscos Content Services Switch serie11000 och 11500. I majoriteten av fallen anges det att felet återfinns på någon hårdvara i kombination med den mjukvara som körs på produkten, till exempel Cisco IOS eller CBOS. I en del fall anges enbart mjukvaran som den felande länken och mer sällan anges att felet enbart gäller någon modell av hårdvaran. Av detta kan man alltså dra slutsatsen att det ofta verkar vara den mjukvara som körs på utrustningen som orsakar sårbarheten. Vid en närmare titt på vilken mjukvara som drabbas mest så är IOS version 11.1-11.2 och 12.0-12.2 mest förekommande.

4.1.4 Linksys

Hos LinkSys utmärker sig speciellt en router, WRT54G [20], då den av de totalt 16 funna sårbarheterna hos tillverkaren står för 8 av dessa. Version 3.01.3 av mjukvaran hos WRT54G är drabbad flest antal gånger följt av version 2.04.4.
Två andra routers som är drabbade av ett flertal sårbarheter är BEFSR41 och BEFVP41 där mjukvara version 1.42.7 och tidigare hos dessa är mest drabbad.

4.1.5 NetGear

Bland Netgears produkter finns det egentligen ingen produkt som är drabbad mer än någon annan. Under senare år sticker dock WGT624 ut lite då alla dess tre sårbarheter dyker upp ungefär samtidigt i mars år 2006.

4.1.6 D-Link

Hos D-Link finns två produkter som förekommer något fler gånger än de andra, DSL-504T och DI 624, båda med tre sårbarheter var. De tre sårbarheter som hittats hos DSL-504T har alla tre blivit registrerade ungefär samtidigt i maj år 2005.

4.1.7 Övriga tillverkare

Produkten OfficeConnect Remote 812 ADSL Router, tillverkad av 3Com, har drabbats av sårbarheter ett antal gånger mellan 2001 och 2004. Redan i augusti 2001 slutade 3Com att ta upp beställningar på denna produkt [24] och rekommenderade istället en annan, förbättrad, variant. Detta är ett bra exempel på att folk faktiskt fortsätter att använda produkter som inte längre tillverkas då det så sent som i augusti 2004, tre år efter att tillverkningen har upphört, fortfarande dök upp sårbarheter hos produkten. En annan produkt som också har drabbats av en del sårbarheter är Belkins 54G Wireless Router, F5D7130.

4.2 Uppkomst och konsekvenser

Orsaken till att en sårbarhet uppstår varierar en hel del. I många fall kan det vara svårt att placera sårbarheten i en speciell kategori och ibland kan det vara svårt att hitta en orsak till att sårbarheten har uppstått överhuvudtaget. Bland de sårbarheter som har blivit kategoriserade av SecurityFocus finns det två grupper som utmärker sig då en majoritet av sårbarheterna återfinns i någon av dessa grupper. Dels är det sårbarheter som kategoriseras in under typen designfel vilket kan innebära allt från fel där utrustningen säljs med standardinställningar för användarnamn och lösenord till problem med förutsägbara TCP Initial Sequence Numbers. I den andra gruppen hamnar sårbarheter där det handlar om att det har uppstått något typ av tillstånd som routern eller switchen inte kan hantera. Vad detta innebär i praktiken varierar från sårbarhet till sårbarhet men exempel på detta kan vara olika typer av flood-attacker eller felaktigt utformade datapaket.

Generellt kan sägas att en hel del sårbarheter uppkommer ur just problem med hanteringen av lösenord och användarnamn. Förutom det allra vanligaste problemet med standardinställningar för användarnamn och lösenord, som nämns ovan, så förekommer bland annat fall där lösenord sparas i klartext eller att produkter levereras utan lösenord överhuvudtaget. En del sårbarheter uppstår också på grund av att det saknas kontroll över längden på den lösenordsträng som skrivs in.

Det är ganska vanligt att fel i routrar och switchar kan kopplas ihop med olika typer av protokoll. Protokoll som tidigare ofta förekommer i dessa sammanhang är ICMP, UDP och HTTP men detta har skiftat lite under åren. ICMP förekommer inte efter år 2002. Den sista sårbarheten där problemet är förutsägbara TCP-sekvensnummer förkommer år 2004. Därefter finns bara tre sårbarheter relaterade till TCP och då är problemet att paketen har utformats på ett felaktigt sätt. UDP förekommer mest mellan år 2001 och 2002 och sedan ytterligare ett antal gånger åren därpå. Sårbarheter relaterade till HTTP och administrationsgränssnitt är däremot lite mer spridda över åren. Detsamma gäller problem relaterade till SNMP som också förekommer någon eller några gånger per år från år 2000 till 2006. Intressant att notera är att det år 2007 knappt finns några sårbarheter relaterade till något specifikt protokoll varken hos routrar eller hos switchar.

Bara ett fåtal sårbarheter kräver lokal åtkomst för att kunna utnyttjas, istället kan sårbarheterna utnyttjas via en attack över nätverket. Hos både routrar och switchar kan de flesta sårbarheterna utnyttjas utan någon speciell kunskap hos angriparen. Endast hos ungefär 15 av 257 sårbarheter har komplexiteten angetts som medium eller hög. En angripare behöver i princip aldrig autentisera sig för att utnyttja sårbarheten, detta förekommer endast i två fall.

4.2.1 Vanliga konsekvenser vid en attack

Den absolut största gruppen av sårbarheter leder, när de blir utnyttjade, till att angriparen kan utföra en DoS-attack. Den andra stora gruppen av sårbarheter är de där angriparen på något vis kan skaffa sig tillgång till systemet, till exempel genom att ta sig förbi autentiseringen, för att sedan ta del av känslig information, som lösenord och inställningar, eller utföra handlingar som han inte borde som till exempel att ändra i konfigurationsfiler. Att en sårbarhet utnyttjas får ofta flera konsekvenser. En attack kan till exempel både leda till överbelastning och en möjlighet att modifiera information. Av de totalt 256 funna sårbarheterna hos routrar och switchar så kan hela 212 stycken av dessa leda till DoS, 116 stycken leder till otillåten visning av information, 59 stycken inkräktar delvis på integritet och tillgänglighet och 52 stycken leder till att angriparen får otillåten tillgång till systemet.

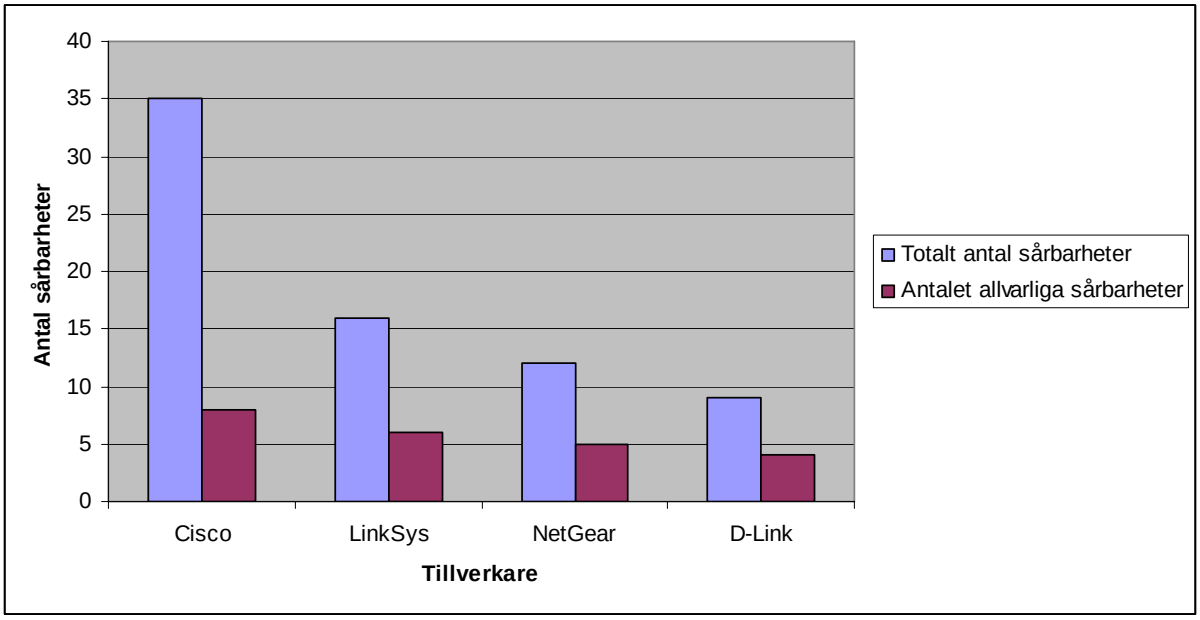
4.2.2 Cisco

Sårbarheter som angriparen kan utnyttja för att utföra en DoS-attack verkar hos Ciscos routrar ha varit ett större problem för några år sedan, speciellt kring år 2001. År 2005-2007 finns bara tre sårbarheter relaterade till DoS. De bakomliggande orsakerna till att dessa sårbarheter har uppstått anges i många fall vara att routern inte kan hantera de tillstånd som uppstår. De senaste tre problemen med DoS har dels drabbat CRS-1 och 1200-serien och operativsystemet där, IOS XR, och dels routrar med operativsystemet IOS 12.1-12.3. Det dessa tre sårbarheter har gemensamt är att sårbarheterna är relaterade till felaktigt utformade MPLS-paket.

Sårbarheterna i 600-serien har gemensamt att de alla fem leder till en DoS-attack om de utnyttjas. Sårbarheterna har alla uppkommit 2001 och gäller dessutom i samtliga fall utom ett operativsystemet CBOS 2.0.1-2.4.2.

En notering rörande Ciscos routrar är att de inte har speciellt många sårbarheter som har en CVSS Base Score över 5.0, bland routrarna 8 stycken av 35, vilket kan ses i Figur 4:1. Detta kan jämföras med Linksys som har 6 stycken sårbarheter med en poäng över 5.0, Netgear som har 5 stycken och D-Link som har 4 stycken. Då Cisco total har mer än dubbelt så många sårbarheter registrerade i NVD som Linksys, tre gånger så många som Netgear och fyra

gånger så många sårbarheter som D-Link så kan man konstatera att Ciscos vid en jämförelse verkar tillverka säkrare produkter.



Figur 4:1 Allvarliga sårbarheter i förhållande till det totala antalet sårbarheter

Extra intressant blir det om man tittar närmare på bara Cisco och Linksys. Linksys ägs också av Cisco men har en målgrupp mer riktade mot små företag och hemanvändare. Linksys köptes upp av Cisco år 2003 [25] och med antagandet att Cisco skulle lägga mer krut på säkerheten än andra tillverkare så borde i så fall antalet allvarliga sårbarheter hos Linksys minska efter att de blev uppköpta av Cisco. Detta visar sig dock inte stämma då 4 av 6 sårbarheter hos Linksys uppkom efter uppköpet. Å andra sidan gäller alla dessa sårbarheter en produkt som började tillverkas redan innan uppköpet varav man kan misstänka att det eventuellt handlar om fel som ”hänger kvar”. Man kan också konstatera att andelen sårbarheter som leder till att angriparen kan ta sig förbi autentiseringen eller ta del av känslig information är större hos Linksys än hos Cisco. En fråga man kan ställa sig är därför om Cisco medvetet väljer att lägga mer resurser på säkerheten när det gäller deras produkter riktade mot större företag. Ett DoS-attack mot utrustningen i ett stort företag drabbar sannolikt väldigt många människor samtidigt jämfört med en attack mot en hemanvändare där det är en enskild individ som drabbas. En missnöjd företagskund drabbar i sin tur Cisco hårdare än vad en missnöjd hemanvändare skulle göra. Man kan också konstatera att det inte finns något fall bland sårbarheterna i NVD, varken hos Ciscos routrar eller hos deras switchar, där en sårbarhet har orsakats av att en produkt har levererats med standardinställningar för användarnamn och lösenord.

Tittar man på Ciscos switchar ser det inte riktigt lika bra ut när det gäller allvarliga sårbarheter. Av totalt 40 sårbarheter hos switcharna har 13 stycken en CVSS Base Score på över 5.0. Tvärtemot routrarna så förekommer det hos switcharna många sårbarheter som kan leda till en DoS-attack, från år 2002 är en majoritet av attackerna av denna typ. Många sårbarheter har också gemensamt att de har orsakats av att det har uppstått ett tillstånd som switchen inte kan hantera, ofta på grund av ett datapaket som är felaktigt utformat. Tidigare var bland annat problem med åtkomstkontrollen en vanlig orsak.

4.2.3 LinkSys

De senaste åren är det nästan uteslutande den trådlösa bredbandsroutern WRT54G som har drabbats av sårbarheter hos Linksys. Denna router är också den produkt som totalt har drabbats av flest sårbarheter av företagets produkter, 8 av 16 sårbarheter handlar om WRT54G. Routern verkar inte bara vara speciellt utsatt utan verkar också ha drabbats av ganska allvarliga sårbarheter. I flera fall handlar det om fel där angriparen kan ta sig förbi autentiseringsprocessen och få tillgång till känslig information. Tre av dessa sårbarheter har en CVSS Base Score på 7.5 vilken räknas som en sårbarhet med hög allvarlighet. WRT54G släpptes första gången år 2003. De sårbarheter som finns registrerade i NVD på denna produkt är nästan alla funna runt samma tidsperiod, augusti och september 2005. Orsakerna till att sårbarheterna har uppstått handlar bland annat om för svag kryptering av konfigureringsinformation i ett fall, i ett annat om att det är möjligt att koppla upp sig utan att använda kryptering och i ett tredje fall om att samma privata nyckel och certifikat används för alla routrar. WRT54G är lite speciell då den har öppen källkod för mjukvaran vilket gör det möjligt för användaren att själv lägga till eller ta bort funktioner. Just detta faktum verkar i sig inte ha bidragit till att det förekommer många sårbarheter på denna produkt. Däremot kan man misstänka att fler sårbarheter har upptäckts just på grund av detta då produkten testas och används på ett annat sätt jämfört med liknande produkter utan öppen källkod.

Linksys produkter verkar generellt drabbas av många sårbarheter där angriparen kan ta del av och, i vissa fall, manipulera information. Denna typ av sårbarhet är hos Linksys lika vanlig som sårbarheter som leder till en DoS-attack.

4.2.4 NetGear

Även Netgear har drabbats av en hel del allvarliga sårbarheter. 5 av totalt 12 stycken sårbarheter hos Netgear har en CVSS Base Score på 7.5 eller högre. Den allvarligaste sårbarheten, med en Base Score på 10.0, finns hos WGT624 som levereras med standardinställningar för användarnamn och lösenord på administratörskontot. Samtidigt som denna sårbarhet upptäcktes dök även en annan sårbarhet upp hos samma produkt vilken innebär att information i vissa fall sparas i klartext. Ännu finns ingen patch till någon av dessa sårbarheter [28][29]. Redan tidigare har det funnits problem med standardinställningar på lösenord och användarnamn men då gällde det produkten RP114.

Hos många av Netgears sårbarheter anges orsaken till sårbarheten vara ett designfel men det finns även ett par fall där orsaken anges vara att det inte sker någon validering av ”input”. Detta har bland andra drabbat FVS318 där två sårbarheter gällande detta dök upp i januari 2005. Inte heller till dessa två sårbarheter finns det några patchar.

4.2.5 D-Link

Även D-Link har ett stort antal sårbarheter med hög CVSS Base Score i förhållande till antalet funna sårbarheter. Fyra av nio stycken sårbarheter har en Base Score på 7.5. Hårdast drabbad av dessa är DSL-504T där det i två fall handlar om att angriparen kan ta sig förbi autenticieringen och i ett fall om att lösenord och användarnamn sparas i klartext.

Precis som hos Linksys är det hos D-Link lika vanligt att sårbarheterna leder till en DoS-attack som till att angriparen får tillgång till systemet eller kan ta del av känslig information.

4.2.6 Övriga tillverkare

3Coms produkt OfficeConnect Remote 812 ADSL Router står för 5 av företagets totalt 8 registrerade sårbarheter i NVD. Orsaken till att sårbarheterna har uppstått anges vara designfel eller att routern inte kan hantera vissa tillstånd som uppstår. Att utnyttja dessa sårbarheter leder bland annat till DoS-attacker och otillåten tillgång till systemet. Värt att notera är också att 3Com efter år 2004 bara har drabbats av 1 sårbarhet.
De 4 sårbarheter som har drabbat HP resulterar alla i en DoS-attack om de utnyttjas och 3 av dem har en CVSS Base Score på 7.8.

4.3 Antal sårbarheter per år och utvecklingen över tiden

Tabell 4:3 visar antalet nya sårbarheter per år i NVD. Tittar man på antalet träffar för sökordet router så ser man att en tydlig ökning sker mellan år 2000 och 2001. En liten nedgång finns år 2002 och framförallt 2003 men sedan stiger antalet funna sårbarheter från år till år. Då antalet sårbarheter för år 2007 i denna rapport bara sträcker sig fram till september är det svårt att jämföra detta år med övriga. Det kan dock vara värt att notera att det i september år 2005 fanns 32 nya sårbarheter registrerade i NVD och i september 2006 30 stycken. Detta skulle kunna tyda på att det år 2007 blir en nedgång i antalet funna sårbarheter då det fram till september 2007 bara finns 19 sårbarheter dokumenterade. Detta är dock något som är svårt att förutse.

Tabell 4:3 Antal sårbarheter per år i NVD

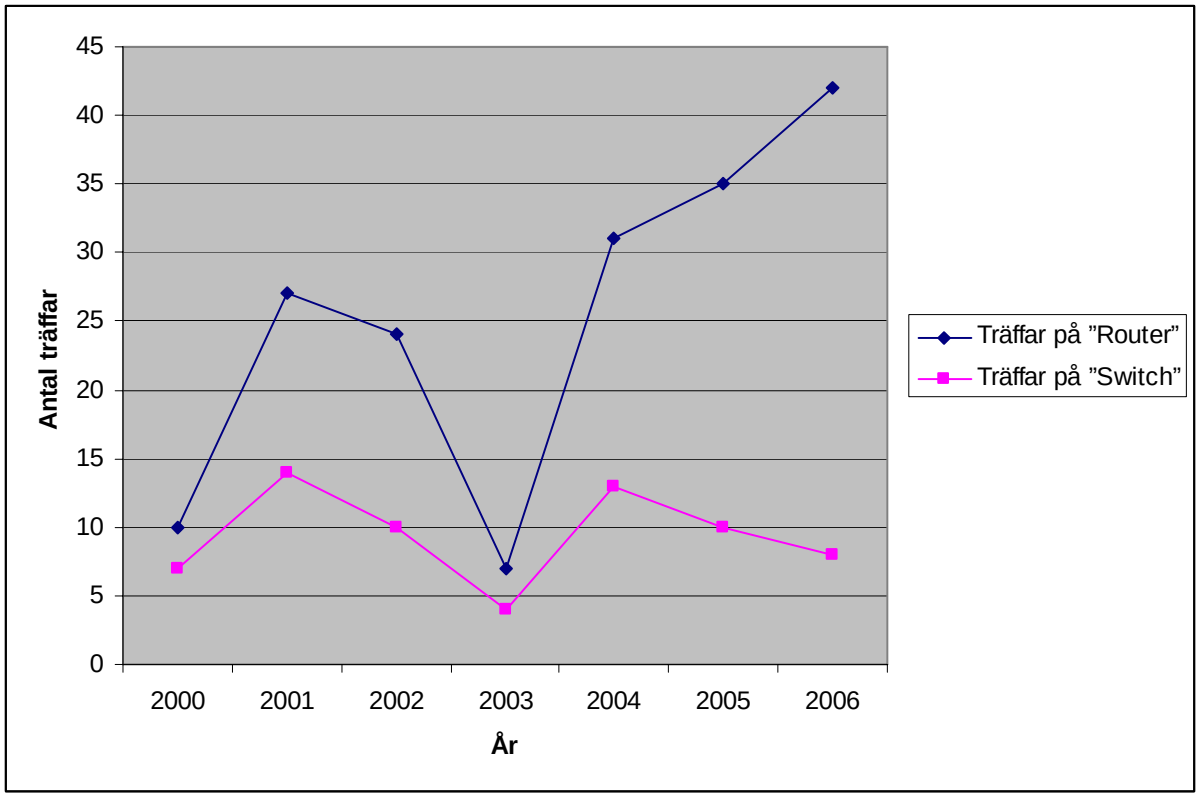
	Träffar på ”Router”	Träffar på ”Switch”	Totalt antal nya sårbarheter
2000	10	7	1017
2001	27	14	1677
2002	24	10	2044
2003	7	4	1456
2004	31	13	2436
2005	35	10	4926
2006	42	8	6600
2007	19 (tom september)	7 (tom september)	5135 (tom september)

När det gäller träffar på sökordet switch så kan man också där se en tydlig ökning mellan år 2000 och 2001 följt av en sänkning 2003 men sedan ligger antalet funna sårbarheter på en ganska konstant nivå. Fram till och med september 2007 finns 7 sårbarheter registrerade på switchar. Troligen ökade denna siffra lite fram till årets slut vilket innebär att 2007 sannolikt kommer att hamna i samma spann som föregående år. Då det rör sig om ett så lågt antal funna sårbarheter per år så är det svårt att se någon klar tendens över tiden.

Det är intressant att se hur liten del av det totala antalet sårbarheter som sårbarheterna i routrar och switchar faktiskt utgör. Som mest är andelen 1,6 % (routrar år 2001) och som minst 0,1 % (switchar år 2007). De flesta år utgör sårbarheterna i routrar respektive switchar någonstans mellan 0,2 % och 0,7 % av det totala antalet sårbarheter. Slår man samman routrar och switchar hittar man toppen år 2004 då de tillsammans står för 1,8 % av alla sårbarheter.

I Figur 4:2 kan man se att det år 2003 sker en tydlig nedgång i antalet träffar. För båda sökorden är det en markant skillnad i träffar mot året före och året efter. Samma sak gäller för det totala antalet träffar i NVD det året, även där kan man se en tydlig skillnad. Denna skillnad kan man även notera i databasen OSVDB [8]. Där hittar man 19 träffar på sökordet

router år 2002, 7 träffar år 2003 och 37 träffar år 2004. Orsaken till att man just år 2003 har ett så lågt antal dokumenterade sårbarheter i förhållande till övriga år är inte helt enkelt att se baserat på informationen i denna undersökning.



Figur 4:2 Antal sårbarheter per år i NVD

En liten del av förklaringen till ökningen från år 2000 till 2001 och minskningen mellan år 2002 och 2003 skulle kunna vara sårbarheterna som rör protokollen TCP, UDP och ICMP. De har alla sin topp runt år 2001 och 2002 och blir sedan allt ovanligare.

Om man tittar på Tabell 4:4 ser man att antalet sårbarheter fördelar sig ganska ojämnt över åren också när det gäller enskilda tillverkare. Cisco har en topp år 2001 med 15 stycken sårbarheter följt av år 2002 och 2006 med 6 respektive 5 sårbarheter. Övriga år hittar man endast ett fåtal sårbarheter. Ett liknande mönster kan man även se hos LinkSys och NetGear. Man kan också notera att dessa tre följer ungefär samma mönster. Hos alla tre sker en nedgång i antalet funna sårbarheter år 2002 och först år 2006 ökar antalet sårbarheter igen. Den höga siffran hos Cisco år 2001 beror till stor del på att alla sårbarheter i deras 600-serie med tillhörande operativsystem CBOS rapporterades in detta år.

Tabell 4:4 Antal sårbarheter per år för tre utvalda tillverkare av routrar

Tillverkare / År	Cisco	LinkSys	NetGear
2000	4	0	0
2001	15	1	0
2002	6	5	4
2003	1	0	0
2004	2	1	1
2005	1	6	2
2006	5	7	8
2007	1	0	0

4.3.1 Generella trender över åren

Det finns en stor variation i vilka typer av sårbarheter som tillverkarna har råkat ut för genom åren men vissa trender och tendenser går att se. År 2000 ledde majoriteten av sårbarheterna till en DoS-attack om de utnyttjades. Året därpå, 2001, var DoS-attackerna inte längre i majoritet. Istället handlade många av sårbarheterna om att angriparen kunde ta del av information eller få otillåten tillgång till systemet. Många av sårbarheterna hos routrarna kategoriseras som designfel. Detta år hittar man också ett antal problem med förutsägbara TCP Initial Sequence Numbers och ett flertal flood-attacker. År 2002 är det en ganska jämn fördelning mellan sårbarheter som leder till DoS-attacker om de utnyttjas och sårbarheter där angriparen får utökade rättigheter. Det förekommer också en del sårbarheter med HTTP-requests som routrarna inte kan hantera och en del DoS-attacker som orsakas av portscanningar. År 2003 är ett år med ett lågt antal sårbarheter men de som finns leder i de flesta fall till DoS-attacker. Även några fall med flood-attacker förekommer. Ett antal lösenordsrelaterade sårbarheter dyker upp år 2004 och dessutom ett antal sårbarheter relaterade till administrationsgränssnitten. Många problem kategoriseras som designfel. Bland switcharna finns en del sårbarheter där problemet är felaktigt utformade datapaket. Problemet med manipulering av paket blir vanligare år 2005. De sårbarheter som leder till DoS-attacker är nästan alla orsakade av felaktigt utformade datapaket. DoS-attackerna är dock i minoritet detta år, istället leder utnyttjade sårbarheter till att angriparna kan ta sig förbi autentiseringar och ta del av känslig information. År 2006 är DoS-attackerna åter ungefär lika vanliga som andra attacker och det förekommer fortfarande problem med manipulerade datapaket. År 2007 förekommer nästan inga DoS-attacker överhuvudtaget hos routrarna men många sårbarheter handlar återigen om att angriparen kan få till gång till systemet och ta del av känslig information. Bland switcharna förekommer däremot i princip bara sårbarheter som leder till DoS-attacker om de utnyttjas.

Problemet med datapaket som angriparen utformar på ett felaktigt sätt för att kunna utföra en attack är ett ständigt återkommande problem. Då man tidigare ofta såg det i samband med ICMP så verkar det på senare år drabba ett antal olika protokoll och utföras på olika sätt och det är därför svårt att hitta någon gemensam nämnare. I väldigt många fall anges sårbarheten enbart bero på just ett ”malformed packet” eller ”crafted packet” i något protokoll, utöver detta ges inga ytterligare detaljer.

4.4 Händelser med påverkan

En händelse som har fått mycket uppmärksamhet i media är den som rör Michael Lynns avslöjande av en allvarlig sårbarhet i Cisco operativsystem IOS. Upptäckten presenterades av Michael Lynn på en Black Hat konferens i juli 2005 och genomfördes trots protester från både Cisco och Internet Security Systems (IIS), företaget där Lynn arbetade när upptäckten gjordes [42]. Lynn avslöjade dock inte några tekniska detaljer som skulle kunna göra det möjligt för en angripare att utnyttja sårbarheten utan att göra egna efterforskningar [41]. I juni 2007 släppte IRM en rapport som tittar mer på sårbarheten i detalj [47], i övrigt är det svårt att hitta någon aktuell information kring händelsen. Något som denna händelse däremot verkar ha bidragit till är diskussioner kring Ciscos hantering av det hela och huruvida Lynn gjorde rätt som genomförde presentationen trots protesterna. En del menar att detta handlade om en så pass allvarlig sårbarhet att det enda rätta var att gå ut och informera folk. Andra anser att Lynn bröt ett förtroende mot IIS och Cisco och att han enbart var ute efter den uppmärksamhet som avslöjandet innebar.

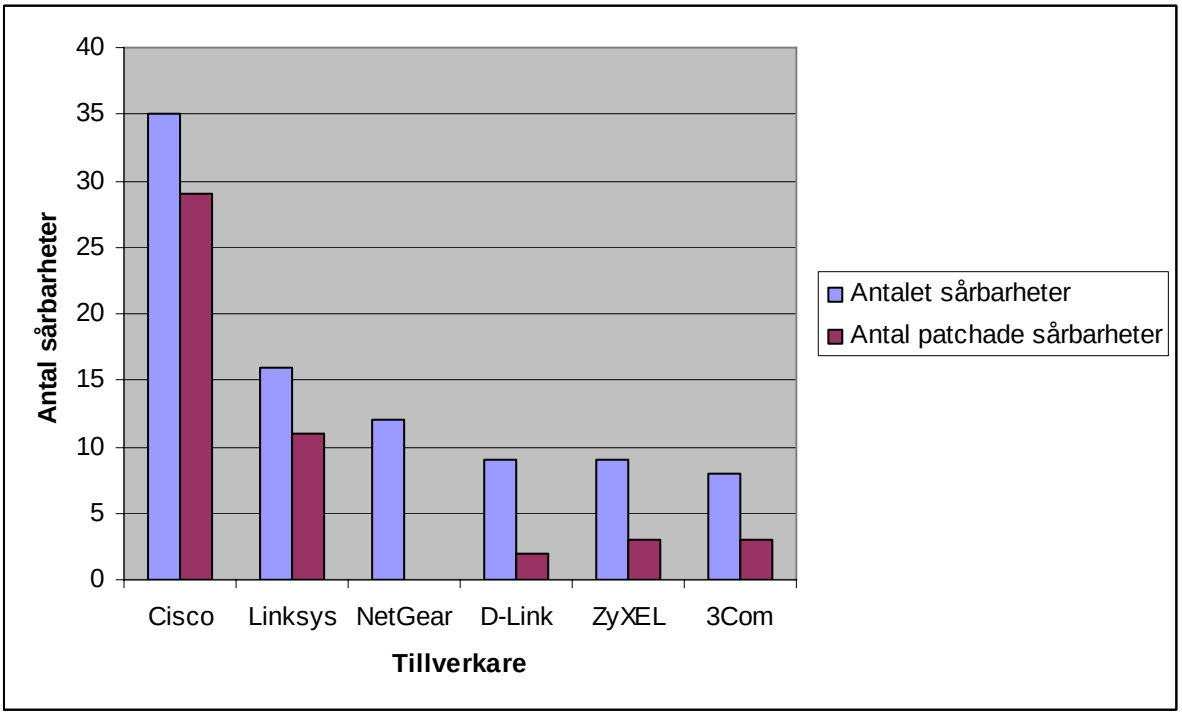
4.5 Buggfixar

Det skiljer sig en hel del mellan de olika företagen när de gäller hanteringen av de sårbarheter som uppstår. Det första man slås av är den information som presenteras på företagens hemsidor. Av de routertillverkare som har drabbats hårdast av sårbarheter; Cisco, Netgear, Linksys, D-Link, Zyxel och 3com så är det bara Cisco som på sin hemsida väljer att tydligt informera om det sårbarheter som har hittats i företaget produkter och vilka åtgärder som har satts in för att komma tillrätta med dessa problem. Dels kan man, på Ciscos hemsida, från varje produktsida, följa en länk till en sida som listar de sårbarheter som har drabbat just den aktuella produkten och dels finns en sida som listar alla säkerhetsfrågor relaterade till Ciscos produkter [35].

På de övriga företagens hemsidor hittas ingen sida likt den hos Cisco som samlar information om alla sårbarheter relaterade till företagets produkter. Däremot kan man hos de flesta tillverkare gå in på en produkt och där få information om vilka buggar olika versioner av dess mjukvara rättar till. Problemet här är att det kan vara svårt för användaren att veta om han har hittat rätt uppdatering då beskrivningarna på tillverkarnas hemsidor ibland är vaga eller kortfattade, till exempel ”Fixed port range issue”. Med en sådan beskrivning är det inte lätt att veta om man faktiskt har hittat rätt uppdatering eller om beskrivningen syftar på lösningen till något helt annat problem än det man är ute efter. Man kan också misstänka att beskrivningen av en sårbarhet ibland skiljer sig åt beroende på vem som tolkar sårbarheten vilket kan bidra till att försvåra identifiering av rätt buggfix. Användaren kanske har läst en beskrivning av felet i någon fristående databas eller mailinglista alternativt har en egen uppfattning om felets orsak och detta kanske inte stämmer överens med tillverkarens beskrivning på hemsidan. För att hitta rätt är den bästa vägen ofta att istället att leta upp sårbarheten i en fristående databas som NVD, SecurityFocus eller X-Force Database [34] där det i de flesta fall finns en bättre beskrivning av sårbarheten samt information och länk direkt till den aktuella buggfixen när en sådan existerar. Man kan dock tycka att detta är en omväg som användaren inte borde behöva ta. Eftersom Cisco väljer att så tydligt beskriva och informera om sårbarheterna så kan man oftast efter en snabb läsning konstatera om man har hittat rätt eller inte.

4.5.1 Patchhantering

För att ta reda på hur bra företagen är på att ta fram patchar till de sårbarheter som förekommer i NVD har jag tittat på uppgifter från både NVD, SecurityFocus och X-Force Database då informationen ibland skiljer sig åt på dessa sidor angående om en buggfix existerar eller inte. Som man kan se i Figur 4:3 så skiljer sig resultatet ganska mycket åt mellan tillverkarna. Allra bäst på att åtgärda sårbarheter är Cisco. Av de 35 sårbarheter som har drabbats deras routrar är det hela 29 stycken som har en patch. Därefter kommer Linksys som har patchar till 11 stycken av totalt 16 sårbarheter. Sedan ser det inte fullt lika bra ut. D-Link och Zyxel har båda 9 sårbarheter var men har bara patchar till 2 respektive 3 av dessa. 3Com har 8 sårbarheter och patchar till 3 av dessa. Allra sämst ser det ut för Netgear som inte har patchar till någon av deras 12 routerrelaterade sårbarheter som finns registrerade i NVD.



Figur 4:3 Patchar till routerrelaterade sårbarheter

En snabb slutsats av detta kan därför vara att Cisco och Linksys, som ägs av Cisco, i större utsträckning verkar satsa på att lösa det problem som dyker upp till skillnad mot övriga företag.

När det gäller Netgear så kan man naturligtvis undra om avsaknaden av buggfixar är något som gäller företagets produkter generellt eller om det är en slump att dessa 12 sårbarheter inte är åtgärdade. Om man på Netgears hemsida tittar närmare på de produkter som återfinns i NVD så listas under de flesta av dessa olika buggar som sägs bli åtgärdade i och med olika uppdateringar av mjukvara tillhörande produkterna. Man kan alltså konstatera att företaget arbetar med att åtgärda buggar, frågan är bara vilket ursprung dessa buggar har? Om det är buggar som företaget själv har hittat och åtgärdat eller om det gäller buggfixar till problem som av någon anledning inte finns med i just NVD men som kanske finns registrerade i andra liknande databaser. Dessa frågor kan även ställas till övriga tillverkare.

4.5.2 Inrapportering av sårbarheter

Information om hur företagen hanterar sårbarheter och eventuellt var ifrån de får information om sårbarheter som drabbar företagets produkter borde man rimligen kunna hitta på företagens hemsidor. Framförallt borde det finnas information om hur man som kund ska gå tillväga för att anmäla en sårbarhet i företagets produkter. Trots en del letande hittas ingen information om detta hos vare sig D-Link, Netgear eller Zyxel. Linksys verkar inte heller ha någon sådan information, däremot anges en speciell mailadress som kan användas för att rapportera om sårbarheter. Risken är att en användare struntar i att rapportera in en såbarhet om han inte hittar vettiga kontaktuppgifter och/eller informationen om hur hanteringen går till. Hos 3Com finns däremot en sida som informerar om hanteringen av sårbarheter samt även ett webbformulär där man kan rapportera in sårbarheter [36]. Även Cisco har en sådan sida, med kontaktinformation samt utförlig information om hur det hanterar inrapporterade sårbarheter [37].

4.5.3 Äldre sårbarheters betydelse för nya sårbarheter

En användare som har en router eller switch idag kanske inte är så speciellt intresserad av att veta att denna produkt för 5 år och 7 uppdateringar sedan drabbades av en sårbarhet rörande till exempel ICMP. Vad användaren däremot antagligen är intresserad av att veta är hur tillverkaren valde att hantera denna sårbarhet. Om tillverkaren har tagit fram en patch till denna sårbarhet, och till alla andra sårbarheter som har dykt upp under åren, är det rimligt att anta att de även kommer att ta fram patchar till de sårbarheter som dyker upp i framtiden. Som användare är man dock inte bara intresserad av att företaget ordnar fram patchar till sårbarheterna, det optimala är ju att det inte förekommer några sårbarheter hos en produkt överhuvudtaget.

En sårbarhet som uppstår på grund av ett nytt och tidigare okänt problem kan vara svårt för tillverkaren att förutse. Däremot borde tillverkarna kunna undvika att drabbas av sårbarheter där problemet är väl känt och där de själva eller någon annan tillverkare redan har drabbats tidigare. Tittar man på sårbarheterna i NVD så visar det sig att så inte alltid är fallet. Enligt Gunter Ollmann, som har skrivit artikeln ”Old Threats Never Die” [45], är problemet att många tillverkare missbedömer tiden under vilken en specifik attack är aktuell. De inser helt enkelt inte att en sårbarhet som en gång väl har uppstått aldrig kommer att försvinna. Istället kommer mängden sårbarheter som en tillverkare måste skydda sig mot att bli allt större. Tillverkarna borde därför hantera äldre sårbarheter och tillhörande patchar, både i egna produkter och sådana som drabbar andra tillverkare, som en viktig källa till kunskap som bör utnyttjas vid utvecklingen av nya produkter.

Ett exempel på att det inte alltid fungerar på detta vis kan ges om man tittar på attacken ”ping of death”. Denna attack blev känd i slutet på 1996 [43] och hade sin topp i juli 1997 [44]. Trots detta så förekommer sårbarheten fortfarande hos Cisco och Zyxel år 2001 och 2002, alltså 4-5 år efter att sårbarheten först blev känd. Uppenbarligen har det hos dessa två tillverkare brustit i hantering av denna sårbarhet. Detta visar också att man aldrig kan förbise en sårbarhet, trots att det var flera år sedan den hade sin topp.

Ur en angripares synvinkel kan äldre sårbarheter vara högst intressanta. Att testa om äldre sårbarheter fortfarande kan utnyttjas kräver inget extra av angriparen och kan dessutom ge bra utdelning. Många användare är av olika anledningar dåliga på att uppdatera sin utrustning med de senaste patcharna [48] vilket är till angriparens fördel. Enligt Gunter Ollman är det också vanligt att äldre sårbarheter återuppstår i samband med att ny mjukvara släpps till en

produkt. Angriparna använder också de patchar som tillverkarna tar fram till sårbarheterna för att ta reda på mer information om sårbarheten. Genom att jämföra koden i det drabbade programmet före och efter att det har blivit patchat kan angriparen se vad som har blivit ändrat och därmed var sårbarheten finns och vad som gjordes för att åtgärda den. Med hjälp av denna information kan angriparen sedan ta fram ett bra sätt att utnyttja sårbarheten [51].

5 Slutsats och framtida arbete

5.1 Slutsatser

Av de totalt 256 sårbarheter som påträffades i NVD vid sökning på "router" och "switch" är Cisco den tillverkare som har drabbats klart flest gånger. Totalt 75 stycken, knappt 30 %, av sårbarheterna har drabbat någon av de produkter som tillverkas under varumärket Cisco. Detta är inte speciellt märkligt då Cisco är marknadsledande både på router- och switchmarknaden. Övriga tillverkare med ett större antal sårbarheter är också dessa tillverkare som hör till de större aktörerna på marknaden. Bland de sårbarheter som har utgjort underlag för analysen förekommer inga fall där en tillverkare med en liten marknadsandel har ett anmärkningsvärt stort antal sårbarheter rapporterade till CVE. Däremot förekommer motsatsen, större tillverkare som bara har ett fåtal sårbarheter inrapporterade till CVE. I stort sett är det så att ett mindre antal tillverkare står för de flesta av sårbarheterna. I det insamlade datat som utgör underlag för denna rapport står 26 % av tillverkarna för 70 % av alla sårbarheterna.

Det är komplext att avgöra hur pass säker en produkt är. Att bara stirra sig blind på den siffra som anger antalet totala sårbarheter kommer inte att ge en rättvis bild. Att vara ett marknadsledande företag innebär att det finns många kunder som använder ens produkter. Dessa kunder använder produkterna på olika sätt efter eget behov vilket innebär en bred bas av människor som alla kan stöta på olika typer av problem. Detta innebär sannolikt att många sårbarheter kommer att upptäckas men inte nödvändigtvis att produkterna har sämre säkerhet än produkterna hos någon annan tillverkare.

Man måste också titta på den källa som uppgifter om sårbarheter hämtas ifrån. Om källan består av 90 % Ciscoanvändare där 3 utav dem dessutom har ett specialintresse för DoS-attacker så kommer detta återspegla sig i statistiken. Så länge källorna inte överensstämmer med hur det ser ut i verkligheten så kommer man inte få fram en helt korrekt bild över vilka tillverkare som drabbas av vilken typ av attacker och hur ofta. Vissa typer av problem är dessutom lättare att upptäcka än andra vilket också kommer visa sig i statistiken. Detta är något man bör ha i bakhuvudet.

Av de studerade sårbarheterna i NVD kan man trots allt dra en del slutsatser:

- Antalet funna sårbarheter i routrar ökar stadigt, bortsett från en svacka 2003. Hos switcharna är kurvan över antalet sårbarheter mer ostadig och har de senaste åren dalat en aning. Sårbarheterna i routrar och switchar står fortfarande för en väldigt liten del av det totala antalet sårbarheter i NVD.

- Juniper och HP har trots sina positioner som tvåor på marknaden inom sina respektive segment bara ett fåtal sårbarheter rapporterade i NVD.

- Attacker som sker med hjälp av felaktigt utformade datapaket är ständigt aktuellt. Runt år 2000-2002 var det vanligt att TCP, UDP och ICMP förekom i dessa sammanhang. Protokollen UDP och TCP förekommer fortfarande ibland men har nu fått sällskap av bland annat MPLS och IKE.

- De vanligaste orsakerna till att sårbarheterna uppstår är designfel eller att det uppstår tillstånd som inte routern kan hantera.

- En utnyttjad sårbarhet leder i majoriteten av fallen till att det angripna systemet blir utsatt för en DoS-attack. På andra plats finns sårbarheter som om det utnyttjas leder till otillåten visning av information.

- De flesta angreppen kan ske via nätverket och det krävs ofta ingen speciell kunskap för att kunna utnyttja sårbarheten.

- Många sårbarheter har sitt ursprung i standardinställningar för användarnamn och lösenord. Det förekommer även sårbarheter som beror på att dessa uppgifter sparas i klartext.

- En del sårbarheter uppstår i samband med det administrationsgränssnitt som används för hantering av utrustningen via webben.

- Cisco är den tillverkare som har drabbats av flest allvarliga sårbarheter, både när det gäller routrar och switchar. Bland routrarna handlar det dock bara om ett par fler allvarliga sårbarheter än hos övriga tillverkare.

- Företagens hantering av de sårbarheter som dyker upp skiljer sig mycket åt mellan olika tillverkare. Medan Cisco och Linksys är ganska bra på att ta fram patchar till de sårbarheter som dyker upp i deras routrar så kan det motsatta sägas om Netgear som inte har patchar till någon av de 12 sårbarheter i deras produkter som förekommer i underlaget till denna rapport.

5.2 Rekommendationer

Det finns många aspekter att ta hänsyn till när det gäller val av nätverksutrustning. Det är inte så enkelt att man bara kan välja ut den tillverkare som har minst antal sårbarheter och köpa någon av deras produkter. Att ett företag har många sårbarheter rapporterade hos sina produkter hänger ofta, men inte alltid, ihop med att de är något av de ledande företagen på marknaden. Många användare innebär ett stort antal människor som kan upptäcka problem.

Man kan konstatera att de flesta tillverkare förr eller senare kommer att drabbas av problem. Med tanke på detta så kan det vara en bra idé att istället för att enbart fokusera på hur ofta en tillverkare har drabbats istället titta på hur tillverkarna väljer att hantera de sårbarheter som uppstår. Om det finns många opatchade sårbarheter hos en produkt kan man misstänka att dessa kommer orsaka problem i framtiden. Det kan också finnas ett värde i att titta på hur snabbt tillverkarna tar fram patchar till de sårbarheter som uppstår. Handlar det om 3 dagar, 3 veckor eller 3 år? Är man ägare av kritisk utrustning som, om den blir attackerad, innebär effekter för ett stort antal människor är det extra viktigt att tänka på just detta. Som användare kan man också fundera över fördelen med att välja en produkt från en tillverkare som inte är marknadsledande. För vissa angripare är syftet med en attack enbart att den ska drabba så många som möjligt. Detta uppnås enklast genom att angripa en produkt med många användare. Därav kan det finnas en poäng i att inte använda just den produkten. Det kan också

vara intressant att titta på hur pass allvarliga tidigare sårbarheter hos en tillverkare har varit. Tillverkare som har drabbats av många allvarliga sårbarheter ger inget bra intryck.

En annan sak man bör tänka på är att stänga av de tjänster man inte använder, som till exempel SNMP eller möjligheten till administration via webben. Man bör också se till att ha en policy för lösenordshantering för att undvika de problem med standardinställningar för lösenord som förekommer till och från. Som användare är det också mycket viktigt att se till att ens utrustning alltid är uppdaterad med de senaste patcharna.

Baserat på de uppgifter som framkommit i denna undersökning så finns det inga verkligt stora skillnader mellan de tillverkare som gör utrustning riktad mot hemanvändare. Ingen av tillverkarna har markant fler sårbarheter än någon annan och antalet allvarliga sårbarheter är också ganska jämt fördelade mellan tillverkarna, även om det ser lite bättre ut för Linksys än övriga. Den punkt där det skiljer sig åt mest är hanteringen av patchar. Netgear ligger sämst till medan Linksys är klart bättre på detta. Detta sammantaget väger det över till Linksys fördel. Å andra sidan är Linksys den som har drabbats av flest sårbarheter bland tillverkarna för hemutrustning och många av sårbarheterna finns hos en och samma produkt, WRT54G. Trots detta, och med tanke på de små skillnader som finns mellan tillverkarna av hemutrustning, är det antagligen bättre att i första hand koncentrera sig på att följa de rekommendationer som ges ovan angående hur man ska hantera sin utrustning än att bekymra sig över vilken tillverkare man ska välja.

Tittar man på utrustning som är riktad mot större företag är det lite svårare att göra någon direkt jämförelse då de företag som främst utgör konkurrenter till Cisco har så få träffar i NVD att en jämförelse därför inte vore rättvis. Om man tittar på det som har framkommit om Cisco i denna rapport framstår inte Ciscos produkter som ett dåligt val. Med tanke på hur stor del av marknaden som Cisco faktiskt har så är inte det stora antalet sårbarheter som hittats i Ciscos produkter jämfört med hos andra tillverkare speciellt uppseendeväckande. Cisco är också bra på att ta fram patchar till de sårbarheter som dyker upp och de har inte heller drabbats av speciellt många allvarliga sårbarheter. Detta innebär dock inte att Cisco är ett självklart val. Man bör fundera över hur man ska använda sin utrustning och att det kan finnas en poäng i att använda en mindre känd tillverkare. Att HP och Juniper faktiskt bara har ett fåtal sårbarheter inrapporterade är intressant och skulle kunna tala för en bättre säkerhet hos dessa tillverkare.

5.3 Framtida arbete

Under arbetets gång har en hel del nya frågor uppstått. Vissa har, främst på grund av tidsbrist, lämnats obesvarade. Förmodligen skulle några av frågorna kunna utgöra grund för ett nytt examensarbete.

Detta arbete har tittat på existerande sårbarheter och fokus har legat på de fall och tillverkare med hög förekomst och där man har kunnat se ett mönster av någon sort. Det vore därför intressant att byta fokus och titta på vilka företag och produkter som inte förekommer i NVD överhuvudtaget eller bara med ett fåtal träffar trots att det kanske är en produkt med många användare. Detta leder oss in på frågan om HP och Juniper. Trots att dessa tillverkare år tvåor på marknaden inom sina segment så har de bara ett fåtal sårbarheter vardera rapporterade i NVD. Är detta ett tecken på att de faktiskt tillverkar säkra produkter? Eller kan det vara helt andra orsaker som ligger bakom det låga antalet sårbarheter hos dessa tillverkare? I rapporten

finns några teorier kring detta men för att få ett bättre svar krävs en mer grundläggande undersökning av de bakomliggande orsakerna.

En annan punkt som vore intressant att titta vidare på är buggfixar. Att Netgear inte verkar ha patchar till någon av de sårbarheter som presenteras i NVD är anmärkningsvärt. Detta är dock något som kräver lite mer efterforskningar. Det kan till exempel finnas en möjlighet att sårbarheterna är patchade trots att de olika databaserna anger att så inte är fallet. För att kunna jämföra vore det också intressant att titta på andra produkter och sårbarheter hos Netgear och se hur det står till med patchar hos dessa. Då det dessutom överlag var lite dåligt med patchar till sårbarheterna hos flera tillverkare - speciellt hos den utrustning som är riktad mot hemanvändare - vore det intressant att titta på om detta är specifikt för just routrar och switchar eller om företagen i allmänhet är dåliga på att åtgärda sårbarheter. Dessutom skulle man kunna titta lite närmare på de sårbarheter som saknar patch för att se om de eventuellt finns någon rimlig orsak till att de inte är patchade.

Det skulle också vara intressant att titta på hur stor andel av det totala antalet sårbarheter som drabbar tillverkarna som blir inrapporterade till CVE. Då Cisco på sin hemsida har tydlig information om de sårbarheter som har drabbat företagets produkter skulle en möjlighet vara att jämföra hur många av de sårbarheter som Cisco rapporterar om på sin hemsida som också går att hitta i CVE. På så vis skulle man få en indikation på hur heltäckande CVE faktiskt är.

Källförteckning

[1] The MITRE Corporation," Common Vulnerabilities and Exposures (CVE)", http://cve.mitre.org/index.html. Senast ändrad 071008.

[2] NIST Computer Security Division, "National Vulnerability Database (NVD)", National Institute of Standards and Technology, Department of Commerce, http://nvd.nist.gov/. Senast ändrad 071016.

[3] Forum of Incident Response and Security Teams (FIRST), "Common Vulnerability Scoring System", http://www.first.org/cvss/cvss-guide.html. Hämtad 071011.

[4] NIST Computer Security Division, "NVD Vulnerability Severity Ratings", http://nvd.nist.gov/cvss.cfm?version=2. Hämtad 071011.

[5] Wikipedia, "Vulnerability (computing)", http://en.wikipedia.org/wiki/Vulnerability_%28computer_science%29. Hämtad 071023.

[6] Andrew Vladimirov, Konstantin Gavrilenko, Andrei Mikhailovsky, Janis Vizulis. *Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions*, McGraw-Hill/Osborne, 2006.

[7] Wikipedia, "Denial-of-service attack", http://en.wikipedia.org/wiki/Denial-of-service_attack. Hämtad 071024

[8] Open Security Foundation, Open Source Vulnerability Database (OSVDB), http://osvdb.org/ Hämtad 071105

[9] Juniper Networks, pressrelease, "Juniper Networks Maintains #2 Market Share Position in Service Provider and High-End Enterprise Routing", http://www.juniper.net/company/presscenter/pr/2006/pr-060522.html Hämtad 071107

[10] Ritsuko Ando, "Juniper seen regaining core router share in 2008", Wireservice news, Reuters, Wednesday June 13, 2007 11:33am EDT http://www.reuters.com/article/companyNewsAndPR/idUSN13335339200706 13 Hämtad 071107

[11] The MITRE Corporation, "CVE - Frequently Asked Questions", http://cve.mitre.org/about/faqs.html#a4, Hämtad 071115.

[12] SecurityFocus, http://www.securityfocus.com/, Hämtad 071116

[13] Technology News, 31 augusti 2006, “HP Achieves #2 Ranking in Ethernet Switch Market for First Half 2006” http://www.mirror99.com/20060831/hp_achieves_2_ranking_in_ethernet_switch_market_for_first_half_faac.jspx Hämtad 071120

[14] Tom Espiner , “HP and Cisco battle over network security”, CNET Networks UK, 13 Februari 2006 13:15 GMT http://news.zdnet.co.uk/security/0,1000000189,39252120,00.htm Hämtad 071121

[15] Dell’Oro Group, 21 November 2006 “Service Provider Router Market Sees Surge in Third Quarter” http://www.delloro.com/news/2006/Rtr112106.htm Hämtad 071121

[16] Cisco Systems , “Routers Compare Products and Solutions”, http://www.cisco.com/en/US/products/hw/routers/products_category_buyers_guide.html Hämtad 071121

[17] NETGEAR, “Routers and Gateways” http://www.netgear.com/Products/RoutersandGateways.aspx?for=All Hämtad 071121

[18] D-Link, “About D-Link”, http://www.dlink.com/corporate/profile/ Hämtad 071121

[19] Linksys, a division of Cisco Systems, “About Linksys” http://www.linksys.com/servlet/Satellite?c=L_Content_C1&childpagename=US%2FLayout&cid=1114633975818&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=7581827773H18 Hämtad 071121

[20] Linksys, a division of Cisco Systems, “Wireless-G Broadband Router”, http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US%2FLayout&cid=1149562300349&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=0034939789B02 Hämtad 071126

[21] Cisco Systems, “End-of-Sale & EoL Announcement for Cisco 627, 675/675E, 677, & 678 ADSL CPE”, http://www.cisco.com/en/US/products/hw/routers/ps295/prod_eol_notice0900aecd8014da51.html Hämtad 071205

[22] Cisco Systems, “End-of-Sale and End-of-Life Announcement for the Cisco SN 5420”, http://www.cisco.com/en/US/products/hw/ps4159/ps2160/prod_eol_notice09186a008032d518.html Hämtad 071205

[23] Wikipedia, “Linksys WRT54G series”, http://en.wikipedia.org/wiki/WRT54G Hämtad 071206

[24] 3Com, ”Support for 3Com® OfficeConnect® Remote 812 ADSL Router” http://www.3com.com/products/en_US/detail.jsp?tab=support&pathtype=support&sku=3CP4144 Hämtad 071213

[25] John G. Spooner, CNET Networks, “Cisco buys Linksys for $500m”, 20 Mars 2003 16:19 GMT http://news.zdnet.co.uk/itmanagement/0,1000000308,2132250,00.htm?r=1 Hämtad 071217

[26] Default Router Password Database, http://www.routerpasswords.com/ Hämtad 071219

[27] Robert McMillan, IDG News Service, “Drive-by Web Attack Could Hit Home Routers”, Torsdag, 15 Februari, 2007 9:00 AM PST, http://www.pcworld.com/article/id,129064/article.html Hämtad 071220

[28] IBM Internet Security Systems, X-Force Database, “NETGEAR WGT624 default admin account”, http://xforce.iss.net/xforce/xfdb/24926 Hämtad 071221

[29] IBM Internet Security Systems, X-Force Database, “NETGEAR WGT624 cleartext configuration backup”, http://xforce.iss.net/xforce/xfdb/24927 Hämtad 071221

[30] IBM Internet Security Systems, X-Force Database, “NETGEAR FVS318 Security Log cross-site scripting” http://xforce.iss.net/xforce/xfdb/18921 Hämtad 071221

[31] IBM Internet Security Systems, X-Force Database, “NETGEAR FVS318 bypass URL filter”, http://xforce.iss.net/xforce/xfdb/18920 Hämtad 071221

[32] Alex Tsow, Markus Jakobsson, Liu Yang, Susanne Wetzel, “Warkitting: the Drive-by Subversion of Wireless Home Routers”, http://www.indiana.edu/~phishing/papers/warkit.pdf Hämtad 071221

[33] NETGEAR, “Guide to Internet Security”, http://kbserver.netgear.com/inquira/default.asp?ui_mode=answer&prior_transaction_id=294993&action_code=5&highlight_info=16777223,4,7&turl=http%3A%2F%2Fkbserver.netgear.com%2Fkb_web_files%2FN101191.asp&answer_id=30810291#__highlight Hämtad 071221

[34] Internet Security Systems, X-Force Database, http://xforce.iss.net/xforce/search.php Hämtad 080107

[35] Cisco Systems, “Products & Services Security Advisories”, http://www.cisco.com/en/US/products/products_security_advisories_listing.html Hämtad 080108

[36] 3Com, “3Com Vulnerability Handling and Disclosure Policy”, http://csoweb4.3com.com/security/ Hämtad 080114

[37] Cisco Systems “Products & Services Security Vulnerability Policy - Cisco Systems” http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html Hämtad 080114

[38] Ed Gubbins, Telephony Online, “The core router race”, 12 Juni 2007 3:56 PM, http://telephonyonline.com/access/commentary/core_router_race_061207/ Hämtad 080208

[39] SANS Institute, “Intrusion Detection FAQ: Using SNMP for Reconnaissance” http://www.sans.org/resources/idfaq/snmp.php Hämtad 080211

[40] Hewlett-Packard, “ProCurve Networking by HP warranty information”, http://www.hp.com/rnd/support/warranty/index.htm Hämtad 080211

[41] Kim Zetter, Wired, “Whistle-Blower Faces FBI Probe”, 07.29.05 http://www.wired.com/politics/security/news/2005/07/68356 Hämtad 080212

[42] Kim Zetter, Wired, “Router Flaw Is a Ticking Bomb”, 08.01.05 http://www.wired.com/politics/security/news/2005/08/68365

[43] Insecure.org, “Ping of Death”, http://insecure.org/sploits/ping-o-death.html Hämtad 080213

[44] Internet Security Systems, “Ping of Death”, http://www.iss.net/security_center/advice/Intrusions/2000012/default.htm Hämtad 080213

[45] Gunter Ollmann, “Old Threats Never Die, IBM ISS 2007, http://www.windowsecurity.com/uplarticle/14/Old-Threats-Never-Die.pdf Hämtad 080213

[46] Wikinvest, “Cisco Systems (CSCO)”, http://www.wikinvest.com/stock/Cisco_Systems_(CSCO) Hämtad 080219

[47] IRM, Gyan Chawdhary, “IOS Exploitation Techniques” http://www.milw0rm.com/papers/166 Hämtad 080223

[48] ZDNet, George Ou , “Is Cisco killing their own reputation?”, http://blogs.zdnet.com/Ou/?p=85 Hämtad 080304

[49] CBR, Kevin Murphy, “Drive-By Pharming Attack Could Hit Home Networks”, 15 Februari 2007 http://www.cbronline.com/article_news.asp?guid=B2D823D1-D77D-471F-96B2-0DED432A0CA2 Hämtad 080304

[50] The MITRE Corporation, “How We Build the CVE List” http://cve.mitre.org/cve/identifiers/build.html#stage2 Hämtad 080305

[51] SecurityFocus , Robert Lemos, “Reverse engineering patches making disclosure a moot choice?” http://www.securityfocus.com/news/11235 Hämtad 080306

COS/CCS 2008-03

www.kth.se