

cert-fi

INFORMATIONSSÄKERHETSÖVERSIKT

14.10.2008

CERT-FI informationssäkerhetsöversikt 3/2008

På sommaren publicerades en sårbarhet som gällde domännamntjänsten. Okorrigerad möjliggör denna sårbarhet att användaren vilseleds eller e-posten dirigeras till fel adress genom att förfalskade uppgifter matas in i DNS-servern för namnuppslagning (cacheminnet).

Till följd av sårbarheten publicerade CERT-FI årets första varning. Sårbarheten fick mycket publicitet i informationssäkerhetsforum, och program uppdaterades snabbt till säkrare versioner. Således hann denna s.k. DNS cache poisoning-sårbarhet inte utnyttjas i någon större utsträckning.

Flera finländska webbserverar innehåll har olovligt ändrats med hjälp av serverprogram sårbarheter. Det är möjligt att webbplatser i angripna serverar har förvanskats eller att skadliga koder har distribuerats via dem.

Nätadresser som används av operatörer som erbjuder skadlig kod har ändrats. En del amerikanska internetoperatörer har vägrat erbjuda förbindelser åt företag med dåligt rykte.

En sårbarhet i namnserverna kan medföra att användaren vilseleds eller e-post kapas.

Domännamnssystemet är en distribuerad databas, med hjälp av vilken servernas namn och domännamnen omvandlas till numerära IP-adresser för att upprätta förbindelse. Även e-postmeddelanden förmedlas med hjälp av uppgifter i namnserverna. För ordet namntjänst används också förkortningen DNS (domain name service).

Det är möjligt att vilseleda användaren, kapa e-posttrafik eller mata in skadlig kod i slutanvändarens dator genom att förvanska DNS-datat.

Om den s.k. A-posten, som anger IP-adressen, förfalskas kunde det medföra att e-posttrafik till populära webbplatser dirigeras till en adress som angriparen önskar. Innehållet som erbjuds via en server som angriparen kontrollerar kunde t.ex. vara ett skadligt program som utnyttjar webbläsarens sårbarhet eller som är maskerat till en programuppdatering, en phishing-

sida som söker användaruppgifter eller en proxy-server med syfte att kapa en applikationssession.

Genom att förfalska MX-poster som används för routning av e-post kunde man vilseleda e-postmeddelandena som är avsedda för visst företag till en server som angriparen kontrollerar.

Genom att förfalska de NS-poster som identifierar domännamnets officiella namnserverar kunde däremot alla DNS-förfrågningar om ett speciellt domännamn dirigeras till en server som angriparen kontrollerar. Angriparen skulle då i praktiken ha kapat all information om domännamn.

DNS Cache Poisoning innebär att förfalskade uppgifter matas in i namntjänstprogrammets cacheminne

Sårbarheter som gällde genomförande av olika delar av namntjänstsystemet publicerades på sommaren. Dessa DNS-sårbarheter gör att resolverar, komponenter för proxy-serverar och det cacheminnet (*cache*) kan utsättas för obehörig bearbetning av en utomstående instans. Denna typ av attack kallas allmänt "*DNS Cache Poisoning*". (Den publicerade) Sårbarheten och upplysningar om hur den kan utnyttjas gör det möjligt att utföra attacken på ett sätt man inte tidigare kände till.

Sårbarheten har att göra med hur DNS-svar identifieras. Angriparen försöker förvanska uppgifter i systemet genom att gissa rätt parametrar för ett DNS-svarspaket. I de sårbara programvarorna har parametrarna inte varit tillräckligt slumpmässiga, och det har därför varit möjligt att gissa sig till dem och sålunda förvränga svaren. Om gissningen är riktig kan angriparen mata in önskat DNS-data i det systems cacheminne som är föremål för attacken. De system som i fortsättningen frågar efter uppgifterna får alltså förfalskade uppgifter som svar.

Endast de användare och datasystem som direkt påverkas av den "förgiftade" namntjänsten, dvs. de som gör rekursiva förfrågningar av en namnserver som innehåller förfalskad information, är utsatta för attacken. Om t.ex. de namnserverar en bredbandsoperatör använder utsattes för en attack, skulle ifrågavarande operatörs alla bredbandskunder påverkas. På motsvarande sätt skulle en namnserver i ett företags interna nät distribuera felaktig infor-

mation till de arbetsstationer som använder servern.

För att avvärja sårbarheten rekommenderade CERT-FI att programvaran skulle uppdateras till en sådan version, där inmatningen av olovlig DNS-data har försvårats genom att den identifierare som hänför sig till förfrågningarna har gjorts slumpmässigare. Dessutom ska rekursiva DNS-förfrågningar tillåtas endast från de nät, som servern kommer att använda för namnutredning.

Än så länge finns ingen egentlig, allmänt använd, inbyggd autentiseringsmodell i namntjänsten, och därför är det fortfarande i teorin möjligt att förfälska svaren. Man försöker dock lindra risken på det sätt som beskrivs ovan. Som en lösning har man föreslagit att DNSSEC-systemet tas i bruk.

Servrar utsatta för sårbarhet söktes på finländska nät

I början av augusti undersökte CERT-FI hur väl finländska domännamns namnservrar som slutar på .fi har skyddats. Vid utredningen testades totalt 4260 namnservrar, och man bedömde samtidigt både skyddet och uppdateringsnivån.

Av de undersökta serverna visade sig 1180 st. (28 %) vara bristfälligt skyddade; de möjliggör rekursiva förfrågningar var som helst på Internet. Av dessa föreföll 602 servrar att inte vara uppdaterade och sålunda potentiella mål för kunna utnyttjas. Rotservrarna för fi-domännamn skyddades genast då en korrigerande uppdatering fanns tillgängliga. De stora teleföretagens servrar skyddades också snabbt.

CERT-FI sände ett informationsbrev till de sårbara servernas ägare. Upprätthållarna uppmanades att installera de senaste informationssäkerhetsuppdateringarna och att överväga om det över huvudtaget är skäl att den autoritära (primära) namnservern för domännamn tillåter rekursiva förfrågningar. Samma undersökning upprepades två veckor efter det att informationsbrevet hade skickats. Som följd av brevet hade det totala antalet sårbara servrar minskat en aning, men fortfarande fanns 491 servrar som föreföll att vara sårbara.

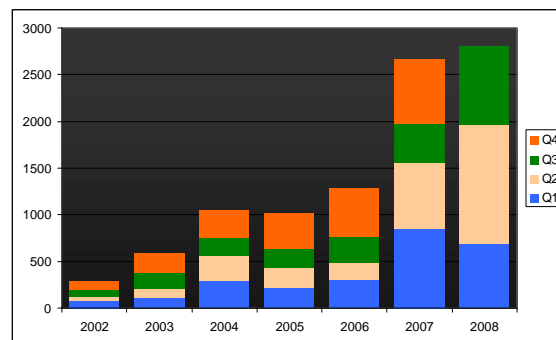
Sårbarheten utnyttjades i Finland

CERT-FI har fått kännedom om ett fall, där namnservrens sårbarhet utnyttjades konkret genom att sårbarheten riktades mot företagets interna näts namntjänst.

Angriparen lyckades mata in en ny A-post med lång giltighetstid (TTL) i cacheminnet till namnservern i företagets interna nät. A-postens namninformation hade en sådan form att företagets webbläsare automatiskt använde den för att definiera webbläsarens cacheminne (s.k. web proxy autodiscovery).

Angriparens definitioner instruerade webbläsaren att använda sig av en proxy-server som angriparen kontrollerade. På det sättet dirigerades webbläsarens all nättrafik via den IP-adress som angriparen definierat.

IP-adressen hänvisade till en angripen webbserver i företagets interna nät, och med hjälp av den försökte man snoka reda på användarens Windows-användaruppgifter och lösenord.



Vid utgången av september månad innevarande år har redan flera händelser registrerats i CERT-FI:s system för hantering av incidenter än under hela föregående år totalt.

Attacker mot webbsidor

Sårbarheter som har hittats i webbservrarnas koder har utnyttjats. Av de servrar som har varit föremål för intrång, och som CERT-FI har fått kännedom om, fanns endast en liten del i Finland.

På sommaren fortsatte den företeelse, som första gången upptäcktes i stor skala denna vår, där webbplatser som är sårbara mot attacker av typ SQL-injektion används för att sprida skadliga program. Också finländska sårbara webbsidor har tidvis använts för missbruk.

En *SQL-injektion* sårbarhet beror på att webbplatsen inte validerar indata och databas inte skyddas tillräckligt noggrant. Då kan det vara möjligt att på en sårbar webbplats eller i den databas webbplatsen använder lagra önskad kod genom att via webbplatsen bygga upp en lämplig SQL-sats. Det är också möjligt att få tillgång till konfidentiell information från den databas webbplatsen använder sig av.

Också *Remote File Inclusion-attacker* har påträffats regelbundet. Ett fel i konfigurationen av webbtillämpningar med programspråket PHP möjliggör attackerna, varvid angriparen kan få servern att lägga till sin egen programkod. Vid angreppen har ny exploit-kod använts, med vilken man bl.a. kan sända skräppost.

Med hjälp av de sårbarheter som har hittats i populär programvara som använts för hantering av webbinnehåll samt underhåll av diskussionsforum och bloggar kan angriparen i vissa fall återinstallera eller ta reda på det lösenord som har använts för administrering av webbtillämpningen. Angriparen har så möjlighet att mata in det innehåll han önskar på webbplatser som använder sårbara tillämpningar. Sårbarheterna har också utnyttjats för attacker mot finländska webbservrar, där servrarna bl.a. har använts som plattformar för phishing-sidor.

En finländsk server distribuerade skadliga program upprepade gånger

CERT-FI fick kännedom om en finländsk webbserver, som upprepade gånger användes för att distribuera skadliga program. Serverns sårbarheter gjorde det möjligt att på nytt och på nytt i servern köra in skadliga program, även om en del av dem också avlägsnades. Under-

sökningarna om upprätthållarens andel i det skedda pågår ännu.

Skadliga program kan också ge sig ut för att vara antivirusprodukt

Flera skadliga program har den senaste tiden kamouflerat sig som antivirusprogram, och på det sättet försökt få användare att installera programmen. De skadliga programmets webbsidor är uppbyggda så att de påminner om antivirusprogramleverantörernas försäljningssidor, som erbjuder såväl kommersiella versioner som gratisversioner. En del av de här sidorna syns enbart om man kommer till dem via en sökmotor.

Det kan vara effektivare att infektera en dator med att locka användaren att själv installera ett skadligt program än att utnyttja sårbarheter i programmen.

Georgien-konflikten påverkade inte de finländska nätens funktionsduglighet

Den beväpnade konflikten i Georgien omfattade också aktivism och nätattacker i datanäten. Attackerna riktade sig bl.a. mot nyhetssidor och politiskt laddade, men inte så viktiga mål med tanke på samhällets funktion. Attackerna hade ingen omedelbar inverkan på de finländska nätens funktion eller säkerhet.

Förändringar i den skadliga webbtrafikens koncentrerings

De skadliga fenomenen på nätet, såsom spridning av skadliga program, de skadliga programmets servrar för lagring av information och botnet-nätverkens kommandoservrar, behöver serverresurser för att fungera effektivt.

Bland hosting-tjänsteleverantörerna finns företag som använder webbadresser där man i genomsnitt hittar mera innehåll eller trafik som kan karakteriseras som skadligt. Företagens nonchalanta linje till kvaliteten på de tjänster kunderna erbjuder kan vara orsaken till att skadliga koder samlas. För någon kan det också vara frågan om en avsiktlig konkurrensfördel.

I samband med incidenter kring skadliga program har en tjänsteleverantör vid namn *Inter-cage*, från San Francisco, och de nätblock företaget administrerar, ofta förekommit. En av

företagets kunder är domännamnleverantören *Estdomains*, som kopplas ihop med många domännamn som använts i skadligt syfte.

Trycket från informationssäkerhets-branschen ledde till att de operatörer som erbjudit nätförbindelser åt Intercage bröt förbindelserna i slutet av september. Estdomains fortsätter sin verksamhet med andra tjänsteleverantörers förbindelser. En del av de webbadresser Intercage använde har övergått till andra tjänsteleverantörer.

Tjänsteleverantören *Russian Business Networks* verksamhet har också granskats tidigare. Företaget finns i S:t Petersburg. I november 2007 försvann RBN från nätet. Det finns emellertid flera tjänsteleverantörer av typ Intercage och RBN som är verksamma för tillfället.

Vissa tjänsteleverantörer är så fokuserade på att erbjuda skadliga koder att det finns skäl att misstänka att arbetsstationer i finländska nät som trafikerar till dessa tjänsteleverantörers adresser har blivit smittade av skadliga program. Varken i Finland eller i de övriga nordiska länderna har någon motsvarande koncentration av skadliga tjänster observerats.

Inom kort publiceras sårbarheter som kan ha långvariga konsekvenser

Den senaste tiden har en sårbarhet, eventuellt förknippad med TCP-protokollet, fått mycket publicitet. Enligt uppgifter i offentligheten skulle denna sårbarhet kunna förorsaka en blockeringsattack redan med små trafikmängder. Tillammans med programtillverkarna och dem som upptäckt sårbarheten koordinerar CERT-FI bedömningen av de verkningar sårbarheten har, eventuella korrigeringsåtgärder och publiceringen. Tilläggsuppgifter om sårbarheter i program publiceras på ett ansvarfullt sätt. Detta innebär att tillverkaren av de sårbara programmen har en möjlighet att korrigera felen innan detaljerna om sårbarheten publiceras.

CERT-FI kontakter	1-3/2008	4-6/2008	7-9/2008	Total	1-9/2007	Ändring
Intervju	17	29	21	67	62	+8%
Sårbarhet eller hot	39	232	52	323	40	+708%
Skadligt program	460	727	532	1719	1286	+34%
Rådgivning	64	87	92	243	280	-13%
Beredning av attack	32	27	12	71	3	+2267%
Dataintrång	14	88	45	147	43	+242%
Blockeringsattack	15	26	31	72	49	+47%
Övriga informationssäkerhetsproblem	10	11	12	33	21	+57%
Social ingenjörskonst	47	36	44	127	167	-33%
Totalt	698	1263	841	2802	1969	+42%

Sårbara webbplatser har aktivt sökts och det syns tydligt också som mängden anmält dataintrång. Anmälningarna om sårbarheter eller hot mot informationssäkerhet har ökat markant jämfört med senaste år.