HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza IISShield alata

CCERT-PUBDOC-2003-07-27

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Zbog velike učestalosti napada na Web poslužitelje, zaštita poslužitelja poželjna je na svim mogućim razinama. Filtriranjem HTTP paketa na aplikacijskoj razini moguće je spriječiti prekide u radu poslužitelja uzrokovane malicioznim paketima. Na taj način poslužitelj se može zaštititi od poznatih metoda napada i neželjenih upita.

Microsoft je s ciljem proširivanja mogućnosti IIS poslužitelja kreirao poseban set API sučelja pod nazivom ISAPI (engl. *Internet Server Application Programming Interface*), omogućujući na taj način programerima izradu jednostavnih ISAPI modula koji unose nove funkcionalnosti u rad poslužitelja.

IISShield ISAPI modul je kvazi-vatrozid, koji na aplikacijskoj razini filtrira neželjene HTTP upite, štiteći na taj način IIS poslužitelj od napada. Korištenjem IISShielda maliciozni paketi se odbacuju prije nego ih poslužitelj uopće pokuša interpretirati, a svaki pokušaj napada upisuje se u vrlo detaljnu log datoteku.

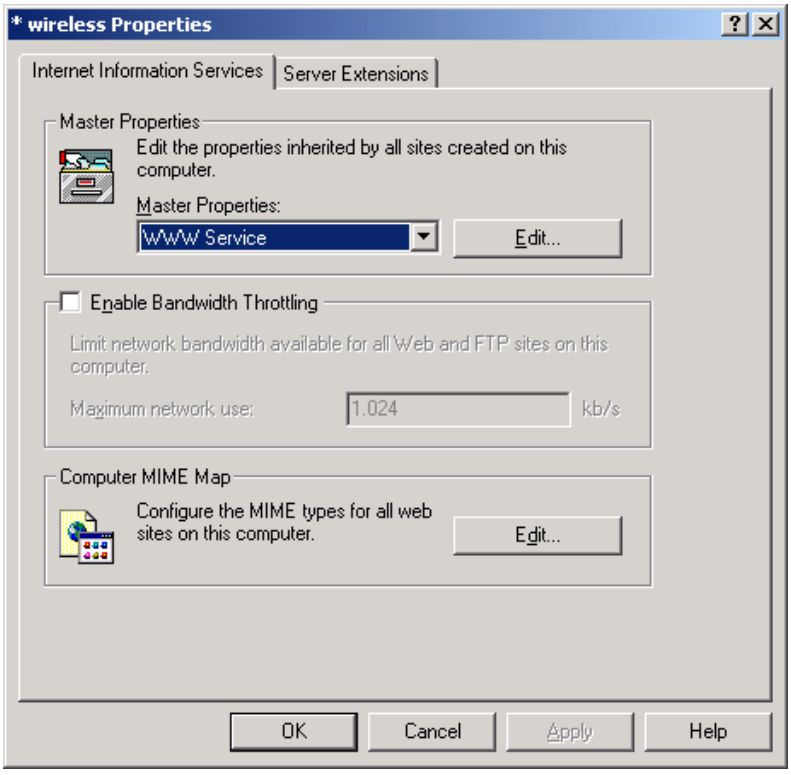
Paket koji sadrži IISShield modul, upute za instalaciju i konfiguraciju, kao i inicijalnu konfiguracijsku datoteku može se dohvatiti na adresi http://www.kodeit.com/tools/iisshield.htm.

2. Instalacija

Paket `iisshield.zip` sadrži datoteke `IISShield.dll` (ISAPI filter), `IISShield.ini` (konfiguracijska datoteka) i datoteke sa uputama za instalaciju i konfiguraciju. Kako bi IISShield ispravno radio, datoteke `IISShield.dll` i `IISShield.ini` moraju biti smještene u isti direktorij.

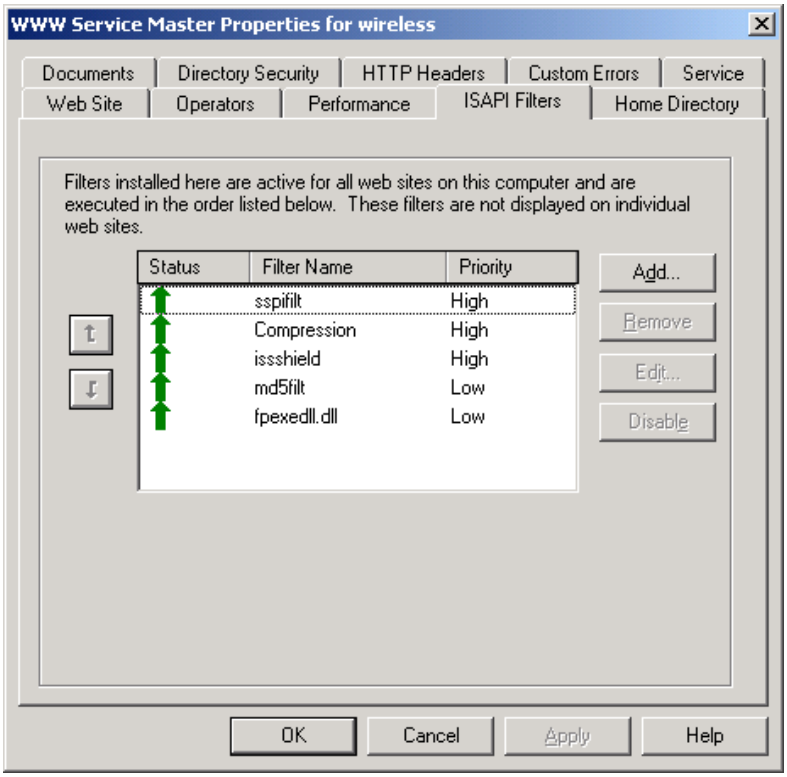
Budući da se ne radi o zasebnoj aplikaciji, već o modulu za IIS poslužitelj, instalacija se svodi na dodavanje novog ISAPI filtra u postavkama IIS poslužitelja. U tu svrhu potrebno je pokrenuti "*Internet Services Manager*" i u lijevom dijelu prozora, desnim klikom miša na ikonu sa imenom računala otvoriti padajući izbornik.

Iz padajućeg izbornika potrebno je odabrati "*Properties*" što će rezultirati otvaranjem prozora prikazanog na slici 1.



Slika 1: "Properties" prozor lokalnog računala unutar Internet Services Manager-a

U sekciji Master Properties, klikom na gumb Edit, otvara se pozor za podešavanje postavki IIS poslužitelja (Slika 2). Unutar kartice ISAPI filters, klikom na gumb Add, dodaju se novi filtri. Novo kreiranom filtru potrebno je dati proizvoljno ime i upisati ispravan put do iisshield.dll datoteke. Nakon toga potrebno je zatvoriti sve dosada otvorene prozore i ponovno pokrenuti IIS poslužitelj, kako bi filtar postao aktivan.



Slika 2: Sučelje za dodavanje ISAPI filtara

Naravno, prije ponovnog pokretanja IIS poslužitelja potrebno je ispravno konfigurirati IISShield vatrozid tj. podesiti parametre u `iisshield.ini` datoteci.

3. Konfiguracija

Konfiguracijski parametri IISShield-a nalaze se u datoteci `IISShield.ini`, a detaljan opis svakog parametra dolazi u paketu s programom (datoteka `config.htm`).
Konfiguracijska datoteka podijeljena je u dva dijela. U prvom dijelu nalaze se globalni konfiguracijski parametri, dok se u drugom dijelu nalaze sekcije koje pobliže određuju funkciju pojedinih konfiguracijskih parametra.
Tako na primjer parametar `DenyUrlSequence` određuje da li će se filtrirati pojedini URL nizovi, dok sekcija `[DenyUrlSequence]` određuje koji će se nizovi filtrirati. Tipičan primjer `[DenyUrlSequence]` sekcije izgleda ovako:

```
[DenyUrlSequence]
..
./
\
:
%
&
```

Inicijalna `IISShield.ini` datoteka dobar je primjer konfiguracijske datoteke postavljene za visoku sigurnosnu razinu zaštite poslužitelja.

3.1. Globalni parametri

Unutar `IISShield.ini` datoteke moguće je koristiti neke od sljedećih konfiguracijskih parametara:

- `VerbAllow` – Ukoliko je parametar uključen (vrijednost 1), kao valjani HTTP zahtjevi smatrati će se samo oni navedeni unutar `[VerbAllow]` sekcije. U slučaju da je vrijednost parametra 0, kao neispravni će biti odbačeni svi HTTP zahtjevi navedeni unutar `[VerbDeny]` sekcije.
- `ValidHttpVersion` - Ukoliko je parametar uključen (vrijednost 1), dozvoljeni će biti samo oni upiti koji koriste inačice HTTP protokola navedene u `[ValidHttpVersion]` sekciji. U protivnome dozvoljene su sve inačice protokola.
- `ValidHostPort` – Ukoliko je parametar uključen propušteni će biti samo oni HTTP zahtjevi čija vrijednost `Host` parametra u zaglavlju ili ime računala i broj porta unutar URI sheme odgovara nekoj od vrijednosti koje su navedene unutar `[ValidHostPort]` sekcije.
- `ExtensionAllow` - Ukoliko je parametar uključen (vrijednost 1), kao valjani HTTP zahtjevi smatrati će se samo oni koji pokušavaju dohvatiti datoteke s nastavkom navedenim unutar `[ExtensionAllow]` sekcije (npr. `.php`, `.asp`, itd.). U slučaju da je vrijednost parametra 0, kao neispravni će biti odbačeni svi zahtjevi za dohvat datoteka čiji su nastavci navedeni unutar `[ExtensionDeny]` sekcije.
- `DenyHeaderName` - Ukoliko je parametar uključen (vrijednost 1), zabranjeni će biti svi upiti koji u svome zaglavlju sadrže riječi navedene u `[DenyHeaderName]` sekciji. U protivnome, ne vrši se provjera zaglavlja.
- `DenyUrlSequence` - Ovaj parametar koristi se za filtriranje upita koji sadrže nepoželjne znakovne nizove definirane unutar `[DenyUrlSequence]` sekcije. Ovim parametrom nisu obuhvaćeni `Query` znakovni nizovi.
- `DenyQuerySequence` – Definira zabranjene znakovne nizove unutar *Query String-a*.
- `AllowDotInUrl` – Ukoliko je parametar uključen, dozvoljeno je korištenje upita koji u sebi sadrže imena datoteka sa više od jedne točke (npr. www.poslužitelj.hr/moja.datoteka.html).
- `RemoveBanner` – Ukoliko je ovaj parametar uključen, ukloniti će se identifikacijska poruka (engl. *Banner*) IIS poslužitelja.
- `ChangeBanner` – Bilo koji tekst upisan unutar ovog parametra, zamijeniti će inicijalnu identifikacijsku poruku (engl. *Banner*) IIS poslužitelja.
- `LogFilesDir` – Specificira direktorij u koji će se smještati log datoteke. Inicijalno, vrijednost ovog parametra pokazuje na direktorij u kojoj se nalazi IISShield.
- `HighPriority` – Ovaj parametar određuje razinu prioriteta koju će IISShield imati pri svome izvršavanju. 0 označava niski prioritet, kod vrijednost 1 označava visoki prioritet izvođenja.
- `Simulate` – Ukoliko je ovaj parametar uključen, IISShield će analizirati promet i bilježiti neispravne upite u log datoteku, ali se paketi neće odbacivati, već će biti proslijeđeni poslužitelju.

Detaljan opis ostalih parametara nalazi se u `Config.htm` datoteci, koja dolazi u paketu s programom.

3.2. Popis konfiguracijskih sekcija

Za pobliže određivanje ponašanja pojedinih konfiguracijskih parametara, moguće je koristiti sljedeće sekcije:

- `[VerbAllow]`
- `[VerbDeny]`
- `[ValidHttpVersion]`
- `[ExtensionAllow]`
- `[ExtensionDeny]`
- `[ValidHostPort]`
- `[DenyHeaderName]`

- [ValidMaxLenByHeader]
- [DenyUrlSequence]
- [DenyQuerySequence]

Tipične primjere sekcija koje određuju ponašanje pojedinih parametara moguće je pronaći u inicijalnoj IISShield datoteci, koja dolazi u paketu s IISShield filtrom.

4. Rad IISShield filtra

Kada se, nakon instalacije IISShield-a, poslužitelj ponovno pokrene, transparentno će se filtrirati svi maliciozni zahtjevi (u skladu s konfiguracijom IISShield-a). Svi pokušaji slanja neželjenih upita bilježiti će se u log datoteku koja se nalazi u istom direktoriju kao i `iisshield.dll` datoteka. Primjer Log datoteke dan je u nastavku:

```
2003-07-20 01:28:04 80.109.254.36 [Unallowed pair host:port found in
host header] [-] [HEAD / HTTP/1.0]
2003-07-20 01:30:31 155.210.12.231 [Incorrect Request Line] [-] [GET
/scripts/nsiislog.dll]
2003-07-20 03:14:00 212.9.7.79 [Request does not contain allowed
verb] [-] [OPTIONS / HTTP/1.1]
2003-07-20 11:10:31 80.109.254.36 [Unallowed pair host:port found in
host header] [-] [HEAD / HTTP/1.0]
2003-07-20 11:12:57 80.109.254.36 [Unallowed pair host:port found in
host header] [-] [HEAD / HTTP/1.0]
2003-07-20 11:22:48 217.229.21.93 [Url does not contain allowed
extension] [-] [GET /c/winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.1]
2003-07-20 11:22:56 217.229.21.93 [Url does not contain allowed
extension] [-] [GET /c/winnt/system32/12345.exe?/c+dir+c:\ HTTP/1.1]
2003-07-20 11:44:15 157.82.151.41 [Unallowed pair host:port found in
host header] [-] [HEAD / HTTP/1.0]
2003-07-20 11:49:09 161.252.2.86 [Url does not contain allowed
extension] [-] [GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u685
8%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%
u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0]
```

Iz ispisa je vidljivo da datoteka sadrži datum i vrijeme kada je upit primljen, izvornu IP adresu upita, razlog zbog kojeg je upit odbačen te cjelovit tekst upita. Na ovaj način vrlo je lako uočiti i pratiti pokušaje kompromitiranja poslužitelja.

5. Zaključak

IISShield je vrlo korisno proširenje Microsoft IIS poslužitelja, koje na aplikacijskoj razini štiti poslužitelj od malicioznih upita. Velik broj konfiguracijskih opcija čini ovaj IIS modul vrlo fleksibilnim i omogućuje korisniku precizno podešavanje razine zaštite poslužitelja. Vrlo jednostavan i pregledan format log datoteke omogućuje lako praćenje log zapisa i detekciju neovlaštenih aktivnosti.
Filtriranje HTTP upita na aplikacijskoj razini jednostavno je za primjenu i vrlo korisno u okruženjima u kojima ne postoji vatrozid, dok se u okruženjima s vatrozidom ovakvo rješenje može iskoristiti kao dodatna razina zaštite.
Rezultati usporedbe mogućnosti IISShield-a i konkurentskih programa iste namjene mogu se pronaći na adresi http://www.kodeit.com/tools/iisshield_compare.htm.