Gebruik van Cisco Secure IDS/NetRanger Custom String Match-handtekeningen voor "Code Red" Worm Remote Buffer Overflow in Microsoft Index Server ISAPI-uitbreiding in IIS 4.0 en 5.0

Inhoud

Inleiding

Eind juli 2003 schatte Computer Economics (een onafhankelijke onderzoeksorganisatie in Carlsbad, Californië) dat de "Code Red" worm bedrijven $1,2 mrd had gekost in herstel van netwerkschade en in verloren productiviteit. Deze schatting steeg significant met de daaropvolgende vrijgave van de krachtigere "Code Red II" worm. Het Cisco Secure Inbraakdetectiesysteem (IDS), een belangrijk onderdeel van de Cisco SAFE-blauwdruk, heeft zijn waarde aangetoond voor het detecteren en beperken van netwerkbeveiligingsrisico's, inclusief de "Code Red"-worm.

Dit document beschrijft een software-update om de exploitatiemethode te detecteren die wordt gebruikt door de "Code Red" worm (zie Handtekening 2 hieronder).

U kunt de hieronder getoonde handtekeningen voor aangepaste tekenreeksen maken om de exploitatie van een bufferoverloop voor webservers met Microsoft Windows NT en Internet Information Services (IIS) 4.0 of Windows 2000 en IIS 5.0 te vangen. Merk ook op dat de indexeringsservice in Windows XP beta ook kwetsbaar is. Het veiligheidsadvies dat deze kwetsbaarheid beschrijft is te vinden op http://www.eeye.com/html/Research/Advisories/AD20010618.html. Microsoft heeft een patch uitgebracht voor deze kwetsbaarheid die kan worden gedownload van http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx.

De handtekeningen die in dit document worden besproken, zijn beschikbaar gekomen in de handtekeningupdate S(5). Cisco Systems raadt aan de sensoren te upgraden naar 2.2.1.8 of 2.5(1)S3-handtekeningupdate voordat deze handtekening wordt geïmplementeerd. Geregistreerde gebruikers kunnen deze handtekeningupdates downloaden via Cisco Secure Software Center. Alle gebruikers kunnen per e-mail en telefoon contact opnemen met Cisco Technical Support via de wereldwijde contactgegevens van Cisco.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Microsoft Windows NT en IIS 4.0
- Microsoft Windows 2000 en IIS 5.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Aangepaste string matching handtekeningen

Er zijn twee specifieke aangepaste string match handtekeningen om dit probleem aan te pakken. Elke handtekening wordt hieronder beschreven en de toepasselijke productinstellingen worden geleverd.

Handtekening 1 — Indexservertoegang met getracht gebruik

Deze handtekening vuurt op een poging tot bufferoverflow op de Indexing Server ISAPI-uitbreiding in combinatie met een poging om shell code aan de server door te geven om bevoorrechte toegang in de oorspronkelijke vorm van de code te verkrijgen. De handtekening vuurt alleen op de poging om shell code door te geven aan de doeldienst in een poging om volledige toegang op het niveau van het SYSTEEM te krijgen. Een mogelijk probleem is dat deze handtekening niet vuurt als de aanvaller niet probeert om een shell code te geven, maar gewoon de bufferoverloop tegen de dienst in een poging om IIS te crashen en een denial of service te creëren.

String

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Productinstellingen

- Voorvallen: 1
- Poort: 80

Opmerking: als je webservers hebt die luisteren op andere TCP-poorten (bijvoorbeeld 8080), moet je een aparte aangepaste string matchen voor elk poortnummer.

- Aanbevolen niveau van alarmernst:
  - Hoog (Cisco Secure Policy Manager)
  - 5 (Unix Director)
- Richting:

  in

Handtekening 2 — Index Server Access Buffer Overflow "Code Red" Worm

De tweede handtekening vuurt op een poging tot bufferoverflow op de Indexing Server ISAPI-uitbreiding gecombineerd met een poging om shell code aan de server door te geven om bevoorrechte toegang te verkrijgen in de verduisterde vorm die de "Code Red" Worm gebruikt. Deze handtekening vuurt alleen op de poging om shell code door te geven aan de doeldienst in een poging om volledige toegang op het niveau van het SYSTEEM te krijgen. Een mogelijk probleem is dat deze handtekening niet vuurt als de aanvaller niet probeert om een shell code te geven, maar gewoon de bufferoverloop tegen de dienst in een poging om IIS te crashen en een denial of service te creëren.

String

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Opmerking: de bovenstaande string bevat geen spaties.

Productinstellingen

- Voorvallen: 1
- Poort: 80

Opmerking: als je webservers hebt die luisteren op andere TCP-poorten (bijvoorbeeld 8080), moet je een aparte aangepaste string matchen voor elk poortnummer.

- Aanbevolen niveau van alarmernst:
  - Hoog (Cisco Secure Policy Manager)
  - 5 (Unix Director)
- Richting:

  in

Raadpleeg voor meer informatie over Cisco Secure IDS Cisco Secure Inbraakdetectie.

Gerelateerde informatie

- Technische ondersteuning - routers
- Cisco Security Advisories
- Cisco Secure Inbraakdetectiepagina
- Technische ondersteuning – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.