Security referentie-informatie

Security Advisories en kennisgevingen zijn te vinden op http://www.cisco.com/go/psirt, samen met aanvullende informatie van het Product Security Incident Response Team (PSIRT).

Beste praktijken

Beveiliging verbeteren op Cisco-routers

Dit document is een informele discussie over bepaalde Cisco-configuratieinstellingen die de netwerkbeheerders moeten overwegen op hun routers te wijzigen, met name op hun grensrouters, om de beveiliging te verbeteren. Dit document gaat over fundamentele, "boilerplate" configuratieopties die vrijwel algemeen toepasbaar zijn in IP-netwerken, en ongeveer een paar onverwachte items waarvan u zich bewust moet zijn.

Cisco IOS-wachtwoordencryptie

Een niet-Cisco bron heeft een programma uitgebracht om gebruikerswachtwoorden (en andere wachtwoorden) te decrypteren in Cisco-configuratiebestanden. Het programma zal geen wachtwoorden decrypteren die met de **bekwame geheime** opdracht zijn ingesteld. De onverwachte zorg die dit programma onder Cisco-klanten heeft veroorzaakt, heeft ons ertoe gebracht te vermoeden dat veel klanten vertrouwen op de wachtwoordencryptie van Cisco voor meer veiligheid dan het is ontworpen om te verstrekken. Dit document verklaart het beveiligingsmodel achter de Cisco-wachtwoordencryptie en de beveiligingsbeperkingen voor die encryptie

SAFE-blauwdruk van Cisco
SAFE is een uitgebreide veiligheidsblauwdruk die organisaties in staat stelt om veilig aan e-business te doen. Gebruik van een modulaire benadering die veiligheidsontwerp, uitrol en beheer vereenvoudigt terwijl netwerken groeien en veranderen, maakt SAFE netwerken beter die op Cisco AVVID (Architecture for Voice, Video en Integrated Data) zijn gebouwd.

Strategieën voor aanvallen, defensie of beperking

Karakterisering en overtrekken van pakketoverstromingen met Cisco-routers

> De aanvallen van Denial of Service (DoS) worden veel op het internet gebruikt. De eerste stap in de reactie op zo'n aanval is om uit te zoeken wat voor een aanval het eigenlijk is. Veel van de meest gebruikte DoS-aanvallen zijn gebaseerd op grote bandbreedte-overstromingen of op andere repetitieve stromen van pakketten. Dit document biedt inzicht in het begrijpen en overtrekken van deze aanvallen.

Strategieën ter bestrijding van het Nimda-virus

Deze index bevat een uitgebreide opsomming van alle technische tips en aanbevelingen voor het beperken van het Nimda-virus.

[Strategieën ter bestrijding van de Code Red Worm]

Deze index bevat een uitgebreide lijst van alle technische tips en aanbevelingen voor de beperking van de gevolgen van de rode worm.

[Strategieën om te beschermen tegen aanvallen (Distributed Denial of Service)]

Dit Witboek bevat een technische beschrijving van hoe een potentiële aanval van het DDoS en voorgestelde methoden voor het gebruik van Cisco IOS software om tegen deze te verdedigen.

[Strategieën om te beschermen tegen UDP: diagnostische poortontkenning van servicestudies]

Dit Witboek bevat een technische beschrijving van hoe een mogelijke UDP diagnostische poortaanval optreedt en voorgestelde methoden voor het gebruik van Cisco IOS-software om deze te verdedigen.

[Strategieën om te beschermen tegen TCP-SYN-ontkenning van serviceaanvallen]

Dit Witboek bevat een technische beschrijving van hoe een mogelijke TCP SYN-aanval optreedt en voorgestelde methoden voor het gebruik van Cisco IOS-software om deze te verdedigen.

[De meest recente in Denial of Service-aanvallen: "Smurfing" Beschrijving en informatie om de effecten te minimaliseren]
Opmerking: De link hierboven wijst naar een externe site die niet wordt onderhouden door Cisco Systems, Inc.

Het verstrekt diepgaande informatie over "smurf" aanvallen, met een nadruk op Cisco routers en hoe de gevolgen van deze aanvallen te verminderen. Sommige informatie is algemeen en houdt geen verband met de specifieke verkoper van keuze van een organisatie; echter, het wordt geschreven met een Cisco-routerfocus. Dit document vormt geen bevestiging van de gevolgen van "smurf"-aanvallen op de uitrusting van andere verkopers; het bevat echter wel informatie over verschillende verkopers .

Overige bronnen

[Cisco-respons op productbeveiliging]

Dit document beschrijft procedures voor foutrapportage en -incidenten - in het bijzonder wat u moet doen als u onder een actieve beveiligingsaanval staat of u denkt dat u binnenkort wordt aangevallen, als u een beveiligingsprobleem hebt met een Cisco-product, als u technische beveiligingsinformatie over een Cisco-product wilt verkrijgen of als u aanvullende vragen hebt over een aangekondigd beveiligingsprobleem met een Cisco-product. De rol van het Cisco Product Security Incident Response Team (PSIRT) bij de verwerking van beveiligingsincidenten wordt uitgelegd.
