

Security Reference Information

Document ID: 20777

Security Advisories and Notices are located at <http://www.cisco.com/go/psirt> along with additional information from the Product Security Incident Response Team (PSIRT).

Best Practices

Improving Security on Cisco Routers

This document is an informal discussion of some Cisco configuration settings that network administrators should consider changing on their routers, especially on their border routers, in order to improve security. This document is about basic, "boilerplate" configuration items that are almost universally applicable in IP networks, and about a few unexpected items of which you should be aware.

Cisco IOS Password Encryption Facts

A non-Cisco source has released a program to decrypt user passwords (and other passwords) in Cisco configuration files. The program will not decrypt passwords set with the **enable secret** command. The unexpected concern that this program has caused among Cisco customers has led us to suspect that many customers are relying on Cisco password encryption for more security than it was designed to provide. This document explains the security model behind Cisco password encryption, and the security limitations of that encryption

SAFE Blueprint from Cisco

SAFE is a comprehensive security blueprint that enables organizations to safely engage in e-business. Using a modular approach that simplifies security design, rollout, and management as networks grow and change, SAFE enhances networks built on Cisco AVVID (Architecture for Voice, Video and Integrated Data).

Strategies for Attack defense, tracking or mitigation

Characterizing and Tracing Packet Floods Using Cisco Routers

Denial of service (DoS) attacks are common on the Internet. The first step in responding to such an attack is to find out exactly what sort of attack it is. Many of the commonly used DoS attacks are based on high-bandwidth packet floods, or on other repetitive streams of packets. This document provides insight into understanding and tracing these attacks.

Strategies to Combat the Nimda Virus

This index provides a comprehensive listing of all technical tips and mitigation recommendations for dealing with the Nimda Virus.

Strategies to Combat the Code Red Worm

This index provides a comprehensive listing of all technical tips and mitigation recommendations for dealing with the Code Red worm.

Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks

This White Paper contains a technical description of how a potential DDoS attack occurs and suggested methods for using Cisco IOS Software to defend against it.

Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks

This White Paper contains a technical description of how a potential UDP Diagnostic Port attack occurs and suggested methods for using Cisco IOS software to defend against it.

Strategies to Protect Against TCP SYN Denial of Service Attacks

This White Paper contains a technical description of how a potential TCP SYN attack occurs and suggested methods for using Cisco IOS software to defend against it.

The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects

Note: The link above points to an external site that is not maintained by Cisco Systems, Inc.

It provides in-depth information regarding "smurf" attacks, with a focus on Cisco routers and how to reduce the effects of these attacks. Some information is general and not related to an organization's particular vendor of choice; however, it is written with a Cisco router focus. This document is not a confirmation of the effects of "smurf" attacks on other vendors' equipment; however, it does contain information about various vendors.

Other Resources

Cisco Product Security Incident Response

This document describes bug reporting and incident response procedures – specifically, what to do if you are under active security attack or you believe that you are about to be attacked, if you have a security problem with a Cisco product, if you want to obtain technical security information about a Cisco product, or if you have additional questions about an announced security issue with a Cisco product. The role of the Cisco Product Security Incident Response Team (PSIRT) in handling security incidents is explained.

Law Enforcement Contacts

This is a document to assist with providing Law Enforcement Contacts. It is by no means extensive, nor necessarily up to date.

All contents are Copyright © 1992—2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 29, 2003

Document ID: 20777
