

Table of Contents

<u>Cisco Security Notice: Cisco Security Notice: W32.BLASTER Worm Mitigation Recommendations</u>	1
<u>Document ID: 44522</u>	1
<u>Revision 1.8 INTERIM</u>	1
<u>For Public Release 2003 August 14 1600 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	2
<u>Detection</u>	2
<u>Symptoms</u>	3
<u>Affected Products</u>	4
<u>Software Versions and Fixes</u>	5
<u>Obtaining Fixed Software</u>	6
<u>Workaround</u>	6
<u>DoS Mitigation</u>	10
<u>Exploitation and Public Announcements</u>	11
<u>Status of This Notice: FINAL</u>	11
<u>Distribution</u>	11
<u>Revision History</u>	12
<u>Cisco Security Procedures</u>	12
<u>Related Information</u>	12

Cisco Security Notice: Cisco Security Notice: W32.BLASTER Worm Mitigation Recommendations

Document ID: 44522

Revision 1.8 INTERIM

For Public Release 2003 August 14 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Details
Detection
Symptoms
Affected Products
Software Versions and Fixes
Obtaining Fixed Software
Workaround
DoS Mitigation
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures
Related Information

Summary

Cisco customers are currently experiencing attacks due to a new worm that is active on the Internet. The signature of this worm appears as UDP traffic to port 69 and high volumes of TCP traffic to port 135 and 4444. Affected customers have been experiencing high volumes of traffic from both internal and external systems. Symptoms on Cisco devices include, but are not limited to high CPU and traffic drops on the input interfaces. This document focuses on both mitigation techniques and affected Cisco products which need software supplied by Cisco to patch properly.

The worm has been referenced by the name "W32.Blaster", "msblast.exe", "Lovsan", "Poza" and "Exploit-DcomRpc". This worm exploits a vulnerability previously disclosed by Microsoft, details of which can be found at <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>.

There are currently two worms that both exploit systems unpatched for MS03-026, which are referred to as Blaster and Nachi. This document focuses on mitigation techniques for Blaster and our other document focusing on Nachi mitigation techniques is located at <http://www.cisco.com/warp/customer/707/cisco-sn-20030820-nachi.shtml>. Both documents should be considered in applying mitigation techniques to deal with these issues.

Details

Details of the worm can be found on Microsoft's web site, <http://www.microsoft.com/technet/security/alerts/msblaster.msp> .

The effects of this worm can be mitigated by blocking the required ports it uses to spread itself, scan for new infections, and propagate the executable code. This document focuses on blocking the spread of the worm, either before or after your internal network is infected. This worm spreads using valid ports, blocking those ports may break existing functionality, such as file sharing, TFTP or Kerberos authentication. As with all network configurations, Cisco recommends you establish documentation of baseline traffic during normal times, and use that to make decisions about blocking ports or traffic in your network. Block ports with caution to avoid disabling functionality in your network. Brief descriptions of the normal usage of these ports is listed below.

TCP port 135 is used for the MS RPC protocol. This is often used to share files on local network segments, and rarely used to share files over WAN segments. This is the port where the initial vulnerability is exploited, initiating a sequence of events that fully infects a machine. Blocking port 135 can prevent initial infections, but may disable existing filesharing functionality within your network.

UDP port 69 is used for TFTP, often used to load new software images or configurations to networked devices. A host infected with the W32.Blaster worm opens up this port to transfer the msblast.exe file from an infected machine to a newly exploited machine. Blocking this port may prevent the spread of the worm from an already infected machine to vulnerable hosts, but may break existing TFTP functionality within your network including some implementations of Voice over IP.

TCP port 4444 is used for Kerberos authentication and Oracle9i communication. A host fully infected with the W32.Blaster worm opens a command shell on this port, allowing the machine to be controlled remotely. Blocking this port may prevent an infected machine from being used for further malicious activities, but may block existing Kerberos authentication functionality or Oracle9i implementations within your network.

TCP and or UDP ports 137, 138, 139 and 593 have vulnerabilities associated with them and may leave hosts open to exploitation, but are not currently known to be directly connected to the spread of the W32.Blaster worm. Cisco recommends that any unneeded ports, particularly those with known vulnerabilities associated with them, should be blocked both inbound and outbound at edge networks to prevent their remote exploitation.

Detection

Using IOS with NetFlow Enabled to Detect Infected Hosts

NetFlow can be a powerful tool to help identify infected hosts. Netflow must be enabled on an interface with the command **ip route-cache flow**. The following example shows infected hosts attempting to infect random systems on a destination port of 135, which shows in the output as 0087. Port 69 is 0045, and port 4444 is 115c.

```
Router>show ip cache flow | include 0087
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.119	06	0B88	0087	1
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.169	06	0BF8	0087	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.63	06	0E80	0087	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.111	06	0CB0	0087	1

```

Fa2/0      XX.XX.XX.204   Fa1/0      XX.XX.XX.95   06 0CA0 0087   1
Fa2/0      XX.XX.XX.204   Fa1/0      XX.XX.XX.79   06 0C90 0087   1

```

Using CatOS with Sup2 and MLS to Detect Infected Hosts

MLS statistics can help track down infected hosts. NetFlow should be enabled in full flow to see source and destination ports, as in the following example, which shows traffic sourced from infected hosts, attempting to infect random systems on destination port tcp 135.

```

Router>(enable)set mls flow full
Router>show mls statistics entry ip dst-port 135

```

Destination IP	Source IP	Last		Used		Stat-Pkts	Stat-Bytes
		Prot	DstPrt	SrcPrt			
XX.XX.XX.28	XX.XX.XX.10	TCP	135	2329	0	0	
XX.XX.XX.58	XX.XX.XX.28	TCP	135	2342	0	0	
XX.XX.XX.141	XX.XX.XX.223	TCP	135	2333	0	0	
XX.XX.XX.189	XX.XX.XX.1	TCP	135	2347	0	0	
XX.XX.XX.12	XX.XX.XX.19	TCP	135	2328	0	0	
XX.XX.XX.245	XX.XX.XX.137	TCP	135	2343	0	0	
XX.XX.XX.29	XX.XX.XX.22	TCP	135	2318	0	0	

CSIDS Signature

If a Cisco Secure Intrusion Detection System is in use, a signature update file is available at <http://www.cisco.com//tacpage/sw-center/ciscosecure/ids/crypto> (registered customers only) .

To reduce false positives on S49, signature 3327 should be set to only inspect port 135, and not 139 or 445.

Alternatively, a custom signature string can be added to address this worm. Brief instructions are included here:

```

Engine STRING.UDP
SigName MS Blast Worm TFTP Request
ServicePorts 69
RegexString \x00\x01[Mm][Ss][Bb][Ll][Aa][Ss][Tt][.][Ee][Xx][Ee]\x00
Direction ToService

```

Symptoms

For symptoms on an infected Microsoft host, refer to the Microsoft bulletin at <http://www.microsoft.com/technet/security/alerts/msblaster.msp> .

Overall network symptoms may manifest as increased load on firewalls, routers and switches due to increased traffic. You may see instability in networks due to increased load. The traffic load generated by this worm is high, but appears to have stabilized after the first 24 hours of infection.

Unexplained network failures may be due to filtering or blocking legitimate services with filters which are too generic — if devices such as routers or IP phones appear to not boot, please check that they still have access to a TFTP server. These devices are not vulnerable to the W32.Blaster worm, but may depend on open TFTP functionality when they boot to load software or configuration files.

Affected Products

To determine if a product is vulnerable, review the list below. If the software versions or configuration information are provided, then only those combinations are vulnerable. This is a list of appliance software which needs patches downloaded from Cisco:

- Cisco Secure ACS Solution Engine, also known as the Cisco Secure ACS Appliance
- Cisco CallManager
- Cisco Building Broadband Service Manager (BBSM)
 - ◆ BBSM Version 5.1
 - ◆ BBSM Version 5.2
 - ◆ HotSpot 1.0
- Cisco Customer Response Application Server (CRA)
- Cisco Personal Assistant
- Cisco Conference Connection (CCC)
- Cisco Emergency Responder

Other Cisco products which run on a Microsoft-based operating system should strongly consider loading the patch from Microsoft at <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>.

This list is not all inclusive, so refer to Microsoft's bulletin if you think you have an affected Microsoft platform.

- Cisco Unity
- Cisco uOne Enterprise Edition
- Cisco Network Registrar (CNR)
- Cisco Internet Service Node (ISN)
- Cisco Intelligent Contact Manager (ICM) (Hosted and Enterprise)
- Cisco IP Contact Center (IPCC) (Express and Enterprise)
- Cisco E-mail Manager (CEM)
- Cisco Collaboration Server (CCS)
- Cisco Dynamic Content Adapter (DCA)
- Cisco Media Blender (CMB)
- TrailHead (Part of the Web Gateway solution)
- Cisco Networking Services for Active Directory (CNS/AD)
- Cisco SN 5400 Series Storage Routers (driver to interface to Windows server)
- CiscoWorks
 - ◆ CiscoWorks VPN/Security Management Solution (CWVMS)
 - ◆ User Registration Tool
 - ◆ Lan Management Solution
 - ◆ Routed WAN Management
 - ◆ Service Management
 - ◆ VPN/Security Management Solution
 - ◆ IP Telephony Environment Monitor
 - ◆ Small Network Management Solution
 - ◆ QoS Policy Manager
 - ◆ Voice Manager
- Cisco Transport Manager (CTM)
- Cisco Broadband Troubleshooter (CBT)
- DOCSIS CPE Configurator
- Cisco Secure Applications
 - ◆ Cisco Secure Scanner

- ◆ Cisco Secure Policy Manager (CSPM)
- ◆ Access Control Server (ACS)
- Videoconferencing Applications
 - ◆ IP/VC 3540 Video Rate Matching Module
 - ◆ IP/VC 3540 Application Server

Software Versions and Fixes

Cisco Secure ACS Solution Engine/Cisco Secure ACS Appliance

Software version 3.2.1 is affected. CiscoSecure ACS Solution Engine Hotfix KB824146, version 3.2(1.20) will resolve this vulnerability by both applying the patch from Microsoft MS03–039, which supercedes patch MS03–026, and adds additional security measures for the underlying operating system by disabling the following ports: TCP/UDP 137,138, 445.

Customers can download this file at http://www.cisco.com/cgi-bin/tablebuild.pl/solution_engine.

Software release 3.2.2 and later include this patch.

To verify which version is installed, and the existence of any hotfixes or patches on your Cisco Secure ACS Solution Engine, check the **System Configuration** menu, then select the **Appliance Upgrade Status** item.

The instructions for upgrading or applying a hotfix to the CiscoSecure ACS Solution Engine are documented at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacsapp/install/admap.htm#1044616, and are included in the Readme.txt file that accompanies the hotfix files.

For additional questions on this process, consult the documentation or contact Technical Support.

Cisco CallManager, Cisco Customer Response Server/Cisco IP Contact Center Express, Cisco Personal Assistant, Cisco Conference Connection, Cisco Emergency Responder

If the operating system version is Win2000 2.4, customers should download and install one of the following options:

- Latest service pack: win–OS–Upgrade–k9.2000–2–4sr5.exe
- Hotfix specifically for this issue: win–K9–MS03–026.exe

Both are available at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>.

Instructions for installing service patches on BBSM can be found at http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/user/use52_05.htm#50416.

Cisco Building Broadband Service Manager

Software is now available on Cisco's website to patch BBSM 5.1, 5.2, and HotSpot 1.0.

- **Cisco BBSM 5.2** Download RPCBufferOverrun.exe from <http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm52> (registered customers only) .
- **Cisco BBSM 5.1** Download RPCBufferOverrun.exe from <http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm51> (registered customers only) .
- **Cisco BBSM HotSpot1.0** Download RPCBufferOverrun.exe from <http://www.cisco.com/cgi-bin/tablebuild.pl/bbsmhs10> (registered customers only) .

Cisco Security Notice: Cisco Security Notice: W32.BLASTER Worm Mitigation Recommendations

Instructions for installing service patches on BBSM can be found at http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/user/use52_05.htm#50416.

Other Windows-based Cisco Products

Customers should download the Security Patch directly from Microsoft and follow the directions for installation at <http://www.microsoft.com/technet/security/bulletin/MS03-026.msp> .

Obtaining Fixed Software

Where Cisco provides the operating system bundled with the product, Cisco is offering free software patches to address these vulnerabilities for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

Customers with service contracts should contact their regular update channels to obtain any software patch containing the feature sets they have purchased. For most customers with service contracts, this means that patches should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com/tacpage/sw-center/>.

Customers whose Cisco products are provided or maintained through a prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with obtaining the free software patch(es).

Customers who purchased directly from Cisco but who do not hold a Cisco service contract, and customers who purchase through third party vendors but are unsuccessful at obtaining fixed software through their point of sale, should obtain fixed software by contacting Cisco Technical Support using the contact information listed below. In these cases, customers are entitled to obtain a patch to a later version of the same release or as indicated by the applicable row in the Software Versions and Fixes table (noted above).

Cisco Technical Support contacts are as follows:

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Refer to <http://www.cisco.com/warp/customer/687/Directory/DirTAC.shtml> for additional Technical Support contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Note: Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade.

Note: Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workaround

This section is focused on mitigation techniques for the W32.Blaster worm using existing Cisco products in your network. These techniques should be applied both inbound and outbound at the edge of network segments if it is determined they will not affect existing network functionality. Affected systems will still be infected and able to spread within contained sections of the network, therefore it is recommended that all affected servers be patched according to Microsoft's recommendations.

Although each of these examples show how to block all affected ports, it may not be necessary to block all ports. If you have no infected hosts within your network, it may be acceptable to only block port 135 at your network edge, this would prevent infection from outside your network without impeding existing TFTP and Kerberos services. Using NetFlow to identify normal traffic flow on your network will aid you in applying these mitigation techniques with the least impact.

General information regarding strategies for protecting against Distributed Denial of Service attacks may be found at <http://www.cisco.com/warp/customer/707/newsflash.html>.



Caution: As with any configuration change in a network, evaluate the impact of this configuration prior to applying the change.

ACL for IOS

This workaround applies to most router platforms unless a platform is mentioned specifically below.

Note: If you are trying to track source addresses, use Sampled NetFlow, rather than "log" statements in ACLs as the high traffic in combination with the log statement can overwhelm the router.

```
! --- block TFTP

access-list 115 deny udp any any eq 69

! --- block W32.Blaster related protocols

access-list 115 deny tcp any any eq 135
access-list 115 deny udp any any eq 135

! --- block other vulnerable MS protocols

access-list 115 deny udp any any eq 137
access-list 115 deny udp any any eq 138
access-list 115 deny tcp any any eq 139
access-list 115 deny udp any any eq 139
access-list 115 deny tcp any any eq 445
access-list 115 deny tcp any any eq 593

! --- block remote access due to W32.Blaster

access-list 115 deny tcp any any eq 4444

! --- Allow all other traffic -- insert
! --- other existing access-list entries here

access-list 115 permit ip any any
interface <interface>
ip access-group 115 in
ip access-group 115 out
```

Note: The worm will attempt to send packets to random IP addresses, some of which may not exist. When that occurs, the router will reply with an "ICMP unreachable" packet. In some cases, replying to a large number of requests with invalid IP addresses may result in degradation of the router's performance. To prevent that from occurring, use the following command:

```
Router(config)# interface <interface>
Router(if-config)# no ip unreachable
```



Caution: Common network configurations, such as certain types of tunnel structures, require the use of "ip unreachable". If the router must be able to send "ICMP unreachable" packets, you can rate limit the number of replies using the following command:

```
Router(config)# ip icmp rate-limit unreachable <millisecond>
```

Beginning with Cisco IOS Software Release 12.0, the default rate limiting is set to two packets per second (500 ms), a value of 2000 ms is commonly used.

Cisco 12000

Receive ACL Feature On a Cisco 12000 (GSR) series router, packets destined to the router's ip addresses are "punted" to the gigabit route processor (GRP) for processing. In order to protect the GRP, receive ACLs (rACLs) can be applied. rACLs filter traffic destined to the GRP and only traffic explicitly permitted is processed by the GRP, denied traffic is dropped. In general, rACLs do not affect transit traffic (traffic flowing through a router), only traffic destined to the router itself.

rACLs are an extremely effective countermeasure for mitigating the effects of excessive attack traffic destined to the GRP. For more information please refer to GSR: Receive Access Control Lists.

VACL on the 6500

Cisco recommends the use of IOS ACLs on the Cisco Catalyst 4000 with a Sup3 and Hybrid and Native configurations of the Cisco Catalyst 6500, however a VACL configuration example is provided for your convenience. Additionally, the use of "no ip unreachable" is recommended.



Caution: As when making any configuration change, use caution when using VACLs in conjunction with IOS ACLs. Be aware that VACLs apply to all traffic within the VLAN, regardless of direction.

To configure:

```
! --- block TFTP

set security acl ip BLASTER deny udp any any eq 69

! --- block vulnerable MS protocols
! --- Blaster related

set security acl ip BLASTER deny tcp any any eq 135
set security acl ip BLASTER deny udp any any eq 135
```

```

! --- Non-blaster related

set security acl ip BLASTER deny tcp any any eq 137
set security acl ip BLASTER deny udp any any eq 137
set security acl ip BLASTER deny tcp any any eq 138
set security acl ip BLASTER deny udp any any eq 138
set security acl ip BLASTER deny tcp any any eq 139
set security acl ip BLASTER deny udp any any eq 139
set security acl ip BLASTER deny tcp any any eq 593

! --- block remote access due to W32.Blaster

set security acl ip BLASTER deny tcp any any eq 4444

! --- Allow all other traffic
! --- insert other existing access-list entries here

set security acl ip BLASTER permit any any

! -- applies both inbound and outbound

commit security acl BLASTER
set security acl map BLASTER <vlans>

```

To verify:

```
show security acl info all
```

To remove:

```
clear security acl BLASTER
commit security acl BLASTER
```

Catalyst 3550

Apply the IOS ACL on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces in both the inbound and/or outbound direction. Ensure 'no ip unreachable' is configured on the interface.

Apply the IOS ACL to Layer 2 interfaces on the switch only if an IOS ACL is not also applied to the input of a Layer 3 interface (an error message is generated upon attempts to do so). For Layer 2 interfaces the IOS ACL is supported on the physical interfaces only and not on EtherChannel interfaces. It can be applied on the inbound direction only.

Catalyst 2950

Apply the IOS ACL to the interface. Note that ACL's are only supported in the inbound direction. To apply ACLs to physical interfaces the enhanced software image (EI) must be installed.

Catalyst 2900XL and 3500XL

These are Layer 2 switches with no Layer 3 access list support.

PIX

The default behavior of the PIX is to block traffic from lower security level interfaces (OUTSIDE) to higher security level interfaces (INSIDE) unless the affected ports and protocols have been explicitly permitted by an access-list or conduit.

In addition, Cisco recommends blocking traffic from higher security level interfaces (INSIDE) to lower security level interfaces (OUTSIDE).

Customers should deny outbound attempts to these ports:

```
access-list acl_inside deny udp any any eq 69
access-list acl_inside deny tcp any any eq 135
access-list acl_inside deny udp any any eq 135
access-list acl_inside deny tcp any any eq 137
access-list acl_inside deny udp any any eq 137
access-list acl_inside deny tcp any any eq 138
access-list acl_inside deny udp any any eq 138
access-list acl_inside deny tcp any any eq 139
access-list acl_inside deny udp any any eq 139
access-list acl_inside deny tcp any any eq 445
access-list acl_inside deny tcp any any eq 593
access-list acl_inside deny tcp any any eq 4444

! --- insert previously configured acl statements here,
! --- or permit all other traffic out

access-list acl_inside permit ip any any
access-group acl_inside in interface inside
```

The corresponding outbound lists may be applied, however, ACLs are strongly recommended in lieu of outbound lists.

DoS Mitigation

The W32.Blaster worm is due to launch TCP SYN attacks against windowsupdate.com, first starting on the 16th of August 2003.

The packets generated by the infected hosts will be destined to the http port (TCP/80) of the IP address that is resolved as windowsupdate.com. The source addresses will be spoofed to random IP addresses from the same B class as the infected host. Therefore, deploying anti-spoofing techniques may help to mitigate the effects of the DoS attack.

The two common anti-spoofing techniques available on Cisco routers are Unicast Reverse Path Forwarding (Unicast RPF) and access-lists.

When Unicast RPF is enabled on an interface, the router will examine all packets received on that interface and will make sure that the source address and the source interface match the interface on which the packet is received, otherwise the packet will be dropped. Refer to the Configuring Unicast Reverse Path Forwarding document for more information about Unicast RPF.

Deploying access-lists for anti-spoofing needs the explicit knowledge of the networks that may legitimately appear as source addresses on a particular interface. Configuring the **ip access-group <acl> in** command on the interface with an access-list that is permitting all authorized networks and denying the rest of the IP address space will drop the spoofed packets on that interface.

For example, on a corporate router that is connected to the internal network of 192.168.1.0/24 via fastethernet0/0, the following access-list can be used for dropping spoofed packets that are originated from this internal network:

```
access-list <access-list> permit 192.168.1.0 0.0.0.255
access-list <access-list> deny any

interface fastethernet 0/0
 ip access-group <access-list> in
```

<access-list> in the above example must be an unused access-list number in the range of 1-99 or 1300-1999 (IP standard access-list range).

Whenever possible, it is recommended to use Unicast RPF instead of access-lists for anti-spoofing measures.

Refer to the Anti-spoofing section of the Improving Security on Cisco Routers document for more information about anti-spoofing.

Exploitation and Public Announcements

This issue is being exploited actively and has been discussed in numerous public announcements and messages. References include:

- <http://www.eeye.com/html/Research/Advisories/AL20030811.html>
- <http://www.cert.org/advisories/CA-2003-20.html>

Status of This Notice: FINAL

This is a final advisory. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory. Should there be a significant, material change in the facts, Cisco may update this advisory.

A stand-alone copy or paraphrase of the text of this security advisory that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This notice will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/customer/707/cisco-sn-20030814-blaster.shtml>. In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com

Future updates of this notice, if any, will be placed on Cisco's worldwide web. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision 1.0	14–August–2003	Initial Public Release
Revision 1.1	15–August–2003	Added section on DoS
Revision 1.2	16–August–2003	Mitigation Added videoconferencing products to affected products list, noted potential impact of port 69 blocking on some voip implementations, added new name of CRS (IPCC Express) to clarify.
Revision 1.3	18–August–2003	CATOS example has been updated with correct command syntax.
Revision 1.4	18–August–2003	Corrected hex translation of port 4444.
Revision 1.5	21–August–2003	Added a paragraph about the Nachi worm to the end of the Summary section.
Revision 1.6	14–October–2003	Cisco Secure ACS Solution Engine added to Affected products, and Software Versions & Fixes.
Revision 1.7	09–December–2003	Wireless LAN Solution Engine removed from the Affected Products section as it is not vulnerable.
Revision 1.8	19–July–2004	Changed link in CSIDS Signature section.

Cisco Security Procedures

If you have any new information that would be of use to us, please send email to psirt@cisco.com.

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco Security Advisories are available at <http://www.cisco.com/go/psirt/>.

Related Information

- [Technical Support – Cisco Systems](#)

