

Table of Contents

<u>Cisco Security Notice: ZOTOB and WORM_RBOT.CBQ Mitigation Recommendations</u>	1
<u>Document ID: 66097</u>	1
<u>Revision 1.2</u>	1
<u>For Public Release 2005 August 18 2100 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Detection</u>	2
<u>Using IOS with NetFlow Enabled to Detect Infected Hosts</u>	2
<u>IDS/IPS Signatures</u>	2
<u>Symptoms</u>	2
<u>Affected Products</u>	3
<u>Software Versions and Fixes</u>	4
<u>Cisco CallManager, Cisco Customer Response Server/Cisco IP Contact Center Express, Cisco Personal Assistant, Cisco Conference Connection, Cisco Emergency Responder</u>	4
<u>Other Windows-based Cisco Products</u>	4
<u>Obtaining Fixed Software</u>	4
<u>Customers with Service Contracts</u>	4
<u>Customers using Third-party Support Organizations</u>	5
<u>Customers without Service Contracts</u>	5
<u>Workarounds</u>	5
<u>General Worm Mitigation</u>	5
<u>ACL for IOS</u>	5
<u>Cisco Security Agent (CSA)</u>	7
<u>Status of This Notice: FINAL</u>	8
<u>Revision History</u>	8
<u>Cisco Security Procedures</u>	8
<u>Related Information</u>	9

Cisco Security Notice: ZOTOB and WORM_RBOT.CBQ Mitigation Recommendations

Document ID: 66097

Revision 1.2

For Public Release 2005 August 18 2100 UTC (GMT)

Please provide your feedback on this document.

- [Summary](#)
- [Details](#)
- [Detection](#)
- [Symptoms](#)
- [Affected Products](#)
- [Software Versions and Fixes](#)
- [Obtaining Fixed Software](#)
- [Workarounds](#)
- [Status of This Notice: FINAL](#)
- [Revision History](#)
- [Cisco Security Procedures](#)
- [Related Information](#)

Summary

Cisco customers are currently experiencing attacks due to new worms and bots that are active on the Internet. The signature of these worms and bots appears as TCP traffic to port 445 as well as traffic to several secondary TCP ports depending on the variant of the worm. 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 that need software supplied by Cisco to patch properly.

These worms and bots have been referenced by the name ZOTOB in multiple variants, WORM_RBOT.CBQ in multiple variants, and by several other names. These worms and bots exploit a vulnerability previously disclosed by Microsoft, details of which can be found at <http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp> .

Cisco has made free software available for the affected products listed in this Notice that require Cisco-distributed updates.

Details

Details of the worms and bots can be found on Microsoft's web site at <http://www.microsoft.com/technet/security/advisory/899588.msp> .

Additional ZOTOB Worm information can be found on the Cisco MySDN site: http://www.cisco.com/en/US/customer/about/security/intelligence/05_08_zotob_worm.html.

The effects of these worms and bots 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. These worms spread using the well known port TCP/445 which makes the worms challenging to stop as blocking this port may impact existing functionality such as file sharing between Microsoft Windows hosts. As with all network configuration, Cisco recommends establishing a network traffic baseline during normal times and using the baseline to make decisions about blocking ports or traffic in the network. Block ports with caution to avoid disabling functionality in the network.

Detection

Using IOS with NetFlow Enabled to Detect Infected Hosts

NetFlow is a technology for obtaining traffic flow information across a network and can 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 445, which shows in the output as the hexadecimal string **01BD**. Other ports used by worm and bot variants are 7778 which is hexadecimal **1E62**, 8888 which is hexadecimal **22B8**, 8594 which is hexadecimal **2192**, 8563 which is hexadecimal **0890**, 7778 which is hexadecimal **1E62**, 33333 which is hexadecimal **8235**, 11173 which is hexadecimal **2BA5**, 8080 which is hexadecimal **1F90**, 6667 which is hexadecimal **1A0B**, and 69 which is hexadecimal **0045**.

The destination port 445 output is most useful at the network edge. Within the network where legitimate connections are using port 445, the other listed ports may be used to correlate the port 445 data and identify infected hosts.

```
Router>show ip cache flow | include 01BD
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.119	06	0B88	01BD	1
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.169	06	0BF8	01BD	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.63	06	0E80	01BD	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.111	06	0CB0	01BD	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.95	06	0CA0	01BD	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.79	06	0C90	01BD	1

IDS/IPS Signatures

If a Cisco Intrusion Detection System or Intrusion Prevention System is in use, the S185 signature update file includes signatures for both the vulnerability and specific worms and bots attempting to exploit it. S185 is available at: <http://www.cisco.com/tacpage/sw-center/ciscosecure/ids/crypto> (registered customers only) .

Symptoms

For symptoms on an infected Microsoft host, refer to the Microsoft Advisory at <http://www.microsoft.com/technet/security/advisory/899588.aspx> .

Overall network symptoms may manifest as increased load on firewalls, routers and switches due to increased traffic. There may be instability in networks due to increased load.

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 that needs patches downloaded from Cisco:

- Cisco CallManager
- Cisco Conference Connection (CCC)
- Cisco Customer Voice Portal (CVP)
- Cisco Emergency Responder (CER)
- Cisco IP Contact Center Express (IPCC Express)
- Cisco IP Interactive Voice Response (IP IVR)
- Cisco IP Queue Manager (IP QM)
- Cisco MeetingPlace
- Cisco Personal Assistant (PA)

Other Cisco products that run on a Microsoft-based operating system should strongly consider loading the security update from Microsoft at <http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp> .

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

- Cisco Unity
- Cisco Building Broadband Service Manager (BBSM)
- Cisco CNS Network Registrar (CNR)
- Cisco Customer Voice Portal
- Cisco ICM Enterprise Edition
- Cisco ICM Hosted Edition
- Cisco IP Contact Center (IPCC) (Express, Enterprise, Hosted, Remote Agent)
- Cisco E-mail Manager (CEM)
- Cisco Web Collaboration Option
- Cisco Collaboration Server Dynamic Content Adapter
- Cisco Media Blender (CMB)
- Cisco IP Interactive Voice Response
- IP Queue Manager
- Cisco Customer Voice Portal
- Cisco Computer Telephony Integration Option
- Cisco Outbound Option
- Cisco Remote Monitoring Suite Option
- Cisco Support Tools
- 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
 - ◆ IP Telephony Environment Monitor
 - ◆ Small Network Management Solution
 - ◆ QoS Policy Manager

- ◆ Voice Manager
- Cisco Transport Manager (CTM)
- Cisco Broadband Troubleshooter (CBT)
- DOCSIS CPE Configurator
- Access Control Server (ACS)
- Videoconferencing Applications
 - ◆ IP/VC 3540 Video Rate Matching Module
 - ◆ IP/VC 3540 Application Server

Software Versions and Fixes

When considering software upgrades, please also consult <http://www.cisco.com/warp/public/707/advisory.html> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) for assistance

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 in the 2000.4.1 train, customers should download and install one of the following options:

- Latest service pack that includes the fix for this issue: win-OS-Upgrade-K9.2000-4-1sr3.exe
- Hotfix specifically for this issue: win-K9-MS05-039.exe

If the operating system version is in the 2000.2.7 train, customers should download and install one of the following options:

- Latest service pack that includes the fix for this issue: win-OS-Upgrade-K9.2000-2-7sr7.exe
- Hotfix specifically for this issue: win-K9-MS05-039.exe

All software is available at <http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des> (registered customers only) .

Other Windows-based Cisco Products

Customers should download the Security Update directly from Microsoft and follow the directions for installation at <http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp> .

Obtaining Fixed Software

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through 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 the upgrade, which should be free of charge.

Customers without Service Contracts

Customers who purchase direct 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 get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC 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

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Workarounds

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

General Worm Mitigation

For general information regarding strategies and technologies for Worm Mitigation, please refer to the Cisco MySDN site: <http://www.cisco.com/en/US/about/security/intelligence/worm-mitigation-whitepaper.html>.

ACL for IOS



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

The access list entries shown below are examples for several of the worm variants now being tracked. New variants using different ports are possible and should be filtered using the information below as examples.

Any added access list entries should be implemented as part of a Transit Access Control List that filters transit and edge traffic at network ingress points.

For more information on tACLs, refer to **Transit Access Control Lists: Filtering at Your Edge**, available at: <http://www.cisco.com/warp/public/707/tacl.html>.

Note: If trying to track source addresses, use Sampled NetFlow, rather than "log" statements in access lists as the high traffic in combination with the log statement can overwhelm the router. The command `show access-list` can be used to determine the hit count against individual access list entries. This data can be used in conjunction with Sampled NetFlow to determine which specific worm variants are attacking the network.

Network Ingress Inbound Filtering

```
! ZOTOB.(A-F)/BOZARI.(A,B)/WORM_RBOT.CBQ
! Block Initial Scanning
! Note: Care must be taken when blocking TCP/445 to ensure that legitimate connections
      are not impacted
access-list 101 deny tcp any any eq 445
!
! ZOTOB.(A-C)
! Block Remote Shell Creation
access-list 101 deny tcp any any eq 8888
!
! ZOTOB.D
! Block Remote Shell Creation
access-list 101 deny tcp any any eq 7778
!
! ZOTOB.E/BOZORI.A
! Block Remote Shell Creation
access-list 101 deny tcp any any eq 8594
!
! ZOTOB.F/BOZORI.B
! Block Remote Shell Creation
access-list 101 deny tcp any any eq 8563
!
! WORM_RBOT.CBQ
! Block Remote Shell Creation
access-list 101 deny tcp any any eq 7778
!
! Permit other traffic here
! Or include other Transit ACL entries
access-list 101 permit ip any any
```

Network Ingress Outbound Filtering

```
!
! ZOTOB.(A-C)
!
! Block Outbound FTP Requests to Attacking FTP Server (where HAHA.exe file exists)
! while permitting legitimate connections
access-list 110 permit tcp <trusted network address block> <trusted network block
wildcard> any eq 33333 established
access-list 110 deny tcp any any eq 33333
!
! Block Outbound IRC Attempts
access-list 110 deny tcp any any eq 8080
!
! ZOTOB.D
! Block Outbound IRC Attempts
! Note: This may block legitimate IRC connections
!
```

```

access-list 110 deny tcp any any eq 6667
!
! Block Outbound FTP Requests to Attacking FTP Server (where HAHA.exe file exists)
! while permitting legitimate connections
access-list 110 permit tcp <trusted network address block> <trusted network block
wildcard> any eq 11173 established
access-list 110 deny tcp any any eq 11173
!
! WORM_RBOT.CBQ/ZOTOB.(E,F)/BOZORI.(A,B)
! Block Outbound TFTP Attempts
access-list 110 permit udp <trusted network address block> <trusted network block
wildcard> <trusted TFTP servers> <trusted TFTP servers wildcard> eq 69
access-list 110 deny udp any any eq 69
!
! Block Outbound Propagation for ZOTOB.(A-F)/BOZARI.(A,B)/WORM_RBOT.CBQ
!
! Note: Care must be taken when blocking TCP/445 to ensure that legitimate connections
!       are not impacted
access-list 110 deny tcp any any eq 445
access-list 110 deny tcp any any eq 7778
access-list 110 deny tcp any any eq 8888
access-list 110 deny tcp any any eq 8594
access-list 110 deny tcp any any eq 8563
access-list 110 deny tcp any any eq 7778
!
! Permit other traffic here
! Or include other Transit ACL entries
!
access-list 110 permit ip any any
!
! Apply the access-lists to the interface
interface <interface>
ip access-group 101 in
ip access-group 110 out

```

Cisco Security Agent (CSA)

Managed CSA

1. In testing Managed CSA version 4.5 with default polices, the protected server did not become infected. There have been no reports of Managed CSA version 4.5 becoming infected. If Global Correlation is enabled, systems that attack several agents will be blocked when trying to make the initial network connection, mitigating widespread DoS situations.
2. In testing Managed CSA version 4.0.3 with default polices, the protected server did not become infected. There have been no reports of Managed CSA version 4.0.3 becoming infected.
3. Managed CSA version 4.0.3 with default polices may become unstable after repeated attacks and reboot.

CSA for Unity and UnityBridge

- In testing CSA 4.0.3.736 version 1.1.5 for Cisco Unity 4.x and CSA 4.0.3.736 version 1.1.4 for Cisco Unity Bridge, the protected server did not become infected but may become unstable and require a reboot to restore normal operation.

CSA for CallManager, Conference Connection, Emergency Responder, and IP Contact Center Express

1. In testing CSA for Cisco CallManager version 2.0(1), the protected server did not become infected. There have been no reports of version 2.0(1) becoming infected. The protected server may become

- unstable after repeated attacks and require a reboot to restore normal operation.
2. In testing CSA for Cisco CallManager version 1.1(10), the protected server was subject to buffer overflow but CSA blocked the subsequent actions of the exploit.

CSA for ICM and IPCC

1. In testing CSA 4.0.3.728 version 1.0(6) for ICM 5.0 and 6.0 servers, the protected server may become infected and may become unstable and require a reboot to restore normal operation.
2. In testing CSA 4.5.1.616 version 2.0(0) for ICM 7.0 servers, the protected server did not become infected but may become unstable and require a reboot to restore normal operation.

CSA for Personal Assistant

- In testing CSA 4.0.3.736 version 1.1.4 for Cisco Personal Assistant, the protected server did not become infected but may become unstable and require a reboot to restore normal operation.

CSA for CVP, CVP VXML Server, and ISN

1. In testing CSA 4.0.3.728 version 1.1(3) for ISN 2.0 and 2.1 servers, the protected server may become infected and may become unstable and require a reboot to restore normal operation.
2. In testing CSA 4.5.0.573 version 2.0(0) for CVP 3.0 and CVP VXML servers, the protected server did not become infected but may become unstable and require a reboot to restore normal operation.

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

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.

Revision History

Revision 1.2	2005–August–19	Link added to "Details" section; "Affected Products" and "Cisco Security Agent (CSA)" sections updated.
Revision 1.1	2005–August–18	Changes made in "Workarounds" and "Obtaining Fixed Software" sections.
Revision 1.0	2005–August–18	Initial public release.

Cisco Security Procedures

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

- **Cisco Security Advisories and Notices**
-

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Aug 19, 2005

Document ID: 66097
