

Table of Contents

<u>Cisco Security Notice: Nachi Worm Mitigation Recommendations</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Revision 1.5</u>	1
<u>Summary</u>	1
<u>Details</u>	2
<u>Detection</u>	3
<u>Using IOS with NetFlow Enabled to Detect Infected Hosts</u>	3
<u>Using CatOS and IOS on Catalyst 6500 and MLS to Detect Infected Hosts</u>	3
<u>CSIDS Signature</u>	4
<u>Symptoms</u>	5
<u>Affected Products</u>	5
<u>Software Version and Fixes</u>	6
<u>Cisco Secure ACS Solution Engine/Cisco Secure ACS Appliance</u>	6
<u>Cisco CallManager, Cisco Customer Response Server/Cisco IP Contact Center Express, Cisco Personal Assistant, Cisco Conference Connection, Cisco Emergency Responder</u>	7
<u>Cisco Building Broadband Service Manager</u>	7
<u>Other Windows-based Cisco Products</u>	7
<u>Obtaining Fixed Software</u>	7
<u>Workarounds</u>	8
<u>Enable Cisco Express Forwarding (CEF)</u>	8
<u>Policy Based Routing for IOS</u>	9
<u>Modular Quality of Service Command Line Interface</u>	10
<u>ACL for IOS</u>	11
<u>Cisco 12000</u>	12
<u>VACL on the 6500</u>	12
<u>Catalyst 3550</u>	13
<u>Catalyst 2950</u>	13
<u>Catalyst 2900XL and 3500XL</u>	13
<u>PIX</u>	13
<u>Cisco Security Agent (CSA)</u>	14
<u>Exploitation and Public Announcements</u>	14
<u>Status of This Notice: INTERIM</u>	14
<u>Distribution</u>	14
<u>Revision History</u>	15
<u>Cisco Security Procedures</u>	16
<u>Related Information</u>	16

Cisco Security Notice: Nachi Worm Mitigation Recommendations

Please provide your feedback on this document.

Revision 1.5

Summary

Details

Detection

- Using IOS with NetFlow Enabled to Detect Infected Hosts

- Using CatOS and IOS on Catalyst 6500 and MLS to Detect Infected Hosts

- CSIDS Signature

Symptoms

Affected Products

Software Version and Fixes

- Cisco Secure ACS Solution Engine/Cisco Secure ACS Appliance

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

- Cisco Building Broadband Service Manager

- Other Windows-based Cisco Products

Obtaining Fixed Software

Workarounds

- Enable Cisco Express Forwarding (CEF)

- Policy Based Routing for IOS

- Modular Quality of Service Command Line Interface

- ACL for IOS

- Cisco 12000

- VACL on the 6500

- Catalyst 3550

- Catalyst 2950

- Catalyst 2900XL and 3500XL

- PIX

- Cisco Security Agent (CSA)

Exploitation and Public Announcements

Status of This Notice: INTERIM

Distribution

Revision History

Cisco Security Procedures

Related Information

Summary

Cisco customers are currently experiencing high volumes of network traffic from both internal and external systems due to a new worm that is active on the Internet. Many of the network issues from this worm are from high volumes of 92 byte ICMP type 8 (echo request) packets. 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 or operating system patches from Microsoft to patch properly.

The worm has been referenced by the name "Nachi." This worm exploits two vulnerabilities previously disclosed by Microsoft, details of which can be found at the following URLs:

<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>

<http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>

There are currently two worms that both exploit systems unpatched for MS03-026, which are referred to as Nachi and Blaster. This document focuses on mitigation techniques for Nachi and our other document focusing on Blaster mitigation techniques is located at <http://www.cisco.com/warp/public/707/cisco-sn-20030814-blaster.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/virus/alerts/nachi.asp> .

The effects of this worm can be mitigated by blocking the required protocols and 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 protocols and ports. Blocking those ports may break existing functionality, such as network monitoring, file sharing, or TFTP. 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.

ICMP protocol type 8, also known as an echo request, is used by the widely known "ping" utility for connectivity testing and network monitoring purposes. Blocking this protocol can prevent the spreading of the worm but may cause some problems in network diagnostics.

TCP port 135 is used for the MS RPC protocol. This port is needed by many RPC based applications that depend on the service such as the Windows Internet Name Services (WINS), DHCP server, Terminal Services and others. This is one port where the initial vulnerability is exploited through the MS RPC DCOM vulnerability described in MS03-026 initiating a sequence of events that fully infects a machine. Blocking port 135 can prevent initial infections, but may disable other functionality within your network.

TCP port 80 is used by the HyperText Transport Protocol (HTTP). This port is primarily used by Worldwide Web Servers (WWW). The Nachi worm attempts to exploit the vulnerability described by MS03-007 to infect a machine. Blocking port 80 can prevent initial infections, but may break web-based applications.

TCP port 707 is used by the worm as a control channel through which commands are passed to download files named **svchost.exe** and **dllhost.exe** from an infected server. Blocking port 707 can prevent infections by preventing the ability to pass the commands to the vulnerable target to download the worm binaries.

UDP port 69 is used by the Trivial File Transport Protocol (TFTP), often used to load new software images or configurations to networked devices. A host infected with the Nachi worm opens up this port to transfer the **svchost.exe** and **dllhost.exe** files 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 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 Nachi 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 scanning IP address space by using ICMP type 8 packets.

```
Router>show ip cache flow | include 0000 0800
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.119	01	0000	0800	1
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.169	01	0000	0800	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.63	01	0000	0800	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.111	01	0000	0800	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.95	01	0000	0800	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.79	01	0000	0800	1

Note: This output will list all icmp type 8 (echo) flows passing through the router and not all ICMP flows seen on this outputs will be worm related. The Nachi infected hosts will be displayed as the source of many flows that are destined to random destinations.

Using CatOS and IOS on Catalyst 6500 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 examples.

Note: Not all ICMP flows seen on these outputs will be worm related. The Nachi infected hosts will be displayed as the source of many flows that are destined to random destinations.

On Hybrid:

```
Router>(enable)set mls flow full
Router>show mls statistics entry ip protocol icmp
```

Destination IP	Source IP	Last		Used		Stat-Pkts	Stat-Bytes
		Prot	DstPrt	SrcPrt			
XX.XX.XX.28	XX.XX.XX.10	ICMP	0	0	0	0	
XX.XX.XX.58	XX.XX.XX.28	ICMP	0	0	0	0	
XX.XX.XX.141	XX.XX.XX.223	ICMP	0	0	0	0	
XX.XX.XX.189	XX.XX.XX.1	ICMP	0	0	0	0	
XX.XX.XX.12	XX.XX.XX.19	ICMP	0	0	0	0	
XX.XX.XX.245	XX.XX.XX.137	ICMP	0	0	0	0	
XX.XX.XX.29	XX.XX.XX.22	ICMP	0	0	0	0	

On Native:

Note: This command will display the flows for all protocols; you need to look for the flows where the protocol is ICMP.

```
Router(config)# mls flow ip full
Router> show mls ip
Displaying Netflow entries in Supervisor Earl
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----
Pkts          Bytes          Age   LastSeen  Attributes
-----
XX.XX.XX.254  XX.XX.XX.14   icmp:0   :0       0   : 0
0
0            821          16:05:30  L3 - Dynamic
XX.XX.XX.254  XX.XX.XX.10   icmp:0   :0       0   : 0
0
0            149          16:05:31  L3 - Dynamic
XX.XX.XX.254  XX.XX.XX.25   icmp:0   :0       0   : 0
0
0            817          16:05:32  L3 - Dynamic
XX.XX.XX.254  XX.XX.XX.10   icmp:0   :0       0   : 0
1040
58240        821          16:05:36  L3 - Dynamic
XX.XX.XX.254  XX.XX.XX.10   icmp:0   :0       0   : 0
0
0            821          16:05:33  L3 - Dynamic
```

CSIDS Signature

If a Cisco Secure Intrusion Detection System is in use, a signature update file is available to registered customers at the following locations:

- For Version 4.x <http://www.cisco.com/cgi-bin/tablebuild.pl/ids4> (registered customers only)
- For Version 3.x <http://www.cisco.com/cgi-bin/tablebuild.pl/ids3-app> (registered customers only)

Cisco Secure IDS Signature 3327 can detect exploit attempts for MS03-026.

To reduce false positives 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
```

Cisco Secure IDS Signature 5364 can detect exploit attempts for MS03-007.

Alternatively, a custom signature string can be added to address this worm.

Brief instructions are included here:

```
Signature Name    = IIS WebDAV Overflow
Engine           = SERVICE.HTTP
AlarmThrottle    = FireOnce
DeObfuscate      = True
Direction        = ToService
HeaderRegex      = [Tt][Rr][Aa][Nn][Ss][Ll][Aa][Tt][Ee][:] [ \t][Ff]
MaxUriFieldLength = 65000
MinHits          = 1
ResetAfterIdle   = 15
```

Symptoms

For symptoms on an infected Microsoft host, please see the Microsoft bulletin at <http://www.microsoft.com/technet/security/virus/alerts/nachi.asp>.

Overall network symptoms might manifest as increased load or memory allocation failures on firewalls, routers, and switches due to increased traffic. You might see instability in networks due to increased load. The traffic load generated by this worm is high.

Unexplained network failures might be due to filtering or blocking legitimate services with filters that are too generic — if devices such as routers or IP phones appear to not boot, verify that they still have access to a TFTP server. These devices are not vulnerable to the Nachi 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 that 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 that run on a Microsoft based operating system should strongly be considered for loading the patches from Microsoft at: <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>.

<http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>

This list is not all inclusive, 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
 - ◆ Wireless Lan Solution Engine
 - ◆ 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 Version 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 above will include this patch.

To verify which version is installed, and the existence of any hotfixes or patches on your Cisco Secure ACS Solution Engine, please 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 here: 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, please consult the documentation or contact the Technical Assistance Center.

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, 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/pcgi-bin/tablebuild.pl/cmva-3des>.

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 and PatchMS03007.exe from <http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm52> (registered customers only)
- **Cisco BBSM 5.1** --- Download RPCBufferOverrun.exe and Patch51MS03007.exe from <http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm51> (registered customers only)
- **Cisco BBSM HotSpot1.0**---Download RPCBufferOverrun.exe and PatchMS03007.exe from <http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsmhs10> (registered customers only)

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

Other Windows-based Cisco Products

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

<http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>

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 the Cisco Technical Assistance Center (TAC) 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 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

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.

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

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

Workarounds

This section is focused on mitigation techniques for the Nachi 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, this may not be necessary. The Nachi worm will first check the reachability of a host by sending ICMP type 8 messages. If ICMP type 8 packets are filtered, the worm will not try to infect hosts. If you have no infected hosts within your network, it may be acceptable to only block ICMP type 8 and TCP port 135 packets at your network edge, this would prevent infection from outside your network without impeding existing 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/public/707/newsflash.html>.



Caution: As with any configuration change in a network, the impact of the change should be evaluated prior to applying the change.

Enable Cisco Express Forwarding (CEF)

Enabling CEF is highly recommended for mitigating the effects of the Nachi worm. Without CEF, the first packet to each destination will be process switched for creating a fast-switching entry. This may have a negative impact on the router performance while switching many packets to random destinations.

Enabling CEF may help to decrease the CPU load and avoid memory allocation failures which resulted from Nachi worm activity.

Policy Based Routing for IOS

The Nachi worm detects the availability of a node by sending ICMP type 8 (echo request) packets before trying to exploit the RPC vulnerability. The size of the ICMP packet is 92 bytes including the IP header.

The following Policy Based Routing (PBR) configuration can be used to match and drop the ICMP type 8 and type 0 packets that are 92 bytes long. The ICMP type 8 packets generated by the ping utility on other operating systems such as Cisco IOS, Windows 2000, Linux and Solaris, have different packet sizes than 92 bytes. This configuration should not filter the packets that are generated by the ping utility on those operating systems.



Caution: Once applied, this configuration may cause all packets to be process switched on hardware switching platforms such as the Catalyst 6500 series and Cisco 12000 GSR, or PBR may not be supported on these platforms. This may significantly impact the performance of those devices and it is therefore not recommended to use this method on hardware switching platforms.



Caution: Enabling Policy Based Routing may effect the performance of your throughput. It is recommended to enable Cisco Express Forwarding (CEF) for improved performance. If CEF is not enabled on the router, it is recommended to have the "IP route-cache policy" command on the interface. This will increase the performance of Policy Based Routing.



Warning: Microsoft Windows tracert utility uses 92 bytes sized ICMP packets. Using PBR to filter those packets will cause tracert utility not to work.



Warning: If you are using IOS code below 12.0(22)S, 12.1(2)T or 12.1(2) please see the following DDTs: CSCdp83614 (registered customers only) Users below these levels of code should use a length match value of 106 (92 bytes for the IP header plus 14 bytes for the MAC frame size) instead of 92.

```
access-list 199 permit icmp any any echo
access-list 199 permit icmp any any echo-reply

route-map nachi-worm permit 10
! --- match ICMP echo requests and replies (type 0 & 8)
match ip address 199

! --- match 92 bytes sized packets
match length 92 92

! --- drop the packet
set interface Null0

interface <incoming-interface>
! --- it is recommended to disable unreachablees
no ip unreachablees

! --- if not using CEF, enabling ip route-cache flow is recommended
ip route-cache policy

! --- apply Policy Based Routing to the interface
ip policy route-map nachi-worm
```

This configuration needs to be applied on all ingress interfaces on the device. If you have no infected hosts internally it may be acceptable to apply it only at your network edge.

Note: By enabling this configuration you may also be dropping some legitimate ICMP type 8 (echo request) packets that are 92 bytes long.

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.

Modular Quality of Service Command Line Interface



Warning: This feature was integrated in 12.2(13)T1 by CSCdw66131 (registered customers only) , and is not available in earlier versions of IOS.



Warning: Microsoft Windows `tracert` utility uses 92 bytes sized ICMP packets. Using MQC to filter those packets will cause `tracert` utility not to work.

The Nachi worm detects the availability of a node by sending ICMP type 8 (echo request) packets before trying to exploit the RPC vulnerability. The size of the ICMP packet is 92 bytes including the IP header.

The following Modular Quality of Service Command Line Interface (MQC) configuration can be used to match and drop ICMP type 8 and type 0 packets that are 92 bytes long. The ICMP type 8 packets generated by the ping utility on other operating systems such as Cisco IOS, Windows 2000, Linux and Solaris, have different packet sizes than 92 bytes. This configuration should not filter the packets that are generated by the ping utility on those operating systems.

```
access-list 199 permit icmp any any echo
access-list 199 permit icmp any any echo-reply

class-map match-all nachi
  match access-group 199
  match packet length min 92 max 92

policy-map drop-nachi
  class nachi
    drop

interface <interface>
```

```
service-policy input drop-nachi
service-policy output drop-nachi
```

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.

If ICMP packets are not filtered by Policy Based Routing as explained above, it may be preferred to block ICMP packets by using access lists. Please note that filtering ICMP packets will cause the widely used ping utility and other similar diagnostic tools not to work.

```
! --- block ICMP
! ---
! --- you do not need to deny ICMP packets if you already filter
! --- them by using PBR
! ---
! --- blocking ICMP packets with access lists will cause ping utility and
! --- other similar diagnostic tools not to work

access-list 115 deny icmp any any echo
access-list 115 deny icmp any any echo-reply

! --- block vulnerable protocols
! --- Nachi related

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

! --- block TFTP

access-list 115 deny udp any any eq 69

! --- 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

! --- 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
```

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, 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 unreachables" 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 ICMP

set security acl ip NACHI deny icmp any any echo
set security acl ip NACHI deny icmp any any echo-reply

! --- block vulnerable protocols
! --- Nachi related

set security acl ip NACHI deny tcp any any eq 135
set security acl ip NACHI deny udp any any eq 135
set security acl ip NACHI deny udp any any eq 69

! --- block worm control channels

set security acl ip NACHI deny tcp any any eq 4444
set security acl ip NACHI deny tcp any any eq 707

! --- Non-Nachi related

set security acl ip NACHI deny tcp any any eq 137
set security acl ip NACHI deny udp any any eq 137
set security acl ip NACHI deny tcp any any eq 138
set security acl ip NACHI deny udp any any eq 138
```

```

set security acl ip NACHI deny tcp any any eq 139
set security acl ip NACHI deny udp any any eq 139
set security acl ip NACHI deny tcp any any eq 445
set security acl ip NACHI deny tcp any any eq 593

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

set security acl ip NACHI permit any any

! -- applies both inbound and outbound

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

```

To verify:

```
show security acl info all
```

To remove:

```
clear security acl NACHI
commit security acl NACHI
```

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



Caution: While using NAT with a limited number of IP addresses in the translation pool, the

translations may not time out if the global address continues to receive traffic. This may happen even if this traffic is blocked by an access list. For more details, refer to Cisco Bug ID CSCec47609 (registered customers only) .

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 icmp any any echo
access-list acl_inside deny icmp any any echo-reply
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 udp any any eq 69
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

! --- 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.

Cisco Security Agent (CSA)

Using the Desktop and Default Server policies within CSA successfully mitigates this vulnerability/worm.

Exploitation and Public Announcements

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

- <http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>
- http://vil.nai.com/vil/content/v_100559.htm

Status of This Notice: INTERIM

This is a INTERIM notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco anticipates issuing updated versions of this notice when there is material change in the facts.

Distribution

This notice will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.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	20 August 2003	Initial Public Release
Revision 1.1	21-August-2003	Corrected download location for IDS signatures, added additional custom signature for WebDav vulnerability detection, added two workarounds (CSA & MQC) and corrected ICMP message type in PBR workaround, corrected command for CAT OS command.
Revision 1.2	30-August-2003	Added a note for using IOS with NetFlow detection, replaced the Using CatOS with Sup2 and MLS to Detect Infected Hosts section with the Using CatOS & IOS on Catalyst 6500 and MLS to Detect Infected Hosts section, corrected the overall network symptoms text in the Symptoms section, added the Enable Cisco Express Forwarding (CEF) workaround section, added a warning to both the Policy Based Routing for IOS section and the Modular Quality of Service Command Line Interface section.
Revision 1.3	13 September 2003	Added a warning to the Policy Based Routing for IOS section.
Revision 1.4	03 October 2003	Added caution statement to PIX
Revision 1.5	14-October-2003	workaround section, Cisco Secure ACS Solution Engine added to Affected products, and Software Versions & Fixes.

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/warp/public/707/sec_incident_response.shtml. 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**
-

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