

SAFE Nimda Attack Mitigation

This document discusses the recently released Concept/Nimda (Nimda) worm/virus and its effect on the network and its hosts. Today a number of technologies are available for use in Cisco System's products that mitigate the worms' detrimental effects. In addition to these technologies, the SAFE blueprint combines security best practices and secure network design to mitigate worms or viruses like Nimda and other attacks. This paper contains much of the same information that is discussed in the Code-Red white paper posted at:

www.cisco.com/go/safe

This is important to note because as new worms are released, the core mitigation techniques tend to stay the same.

Nimda Background and Function

The Nimda worm is actually a hybrid, containing both worm characteristics and virus characteristics. Both worms and viruses spread and infect multiple systems. The differentiator between the two is that viruses require some form of human intervention to spread. Nimda spreads via the following mechanisms through:

- E-mail as an attachment (virus)
- Network shares (worm)
- JavaScript by browsing compromised Web sites (virus)
- Infected hosts actively scanning for additional exploitable hosts (worm)
- Infected hosts actively scanning for backdoors created by the Code-Red and sadmind/IIS worms (worm)

Nimda, unlike Code-Red, has yet to exhibit intentional destructive capabilities. To date, its activities have been restricted to its self-propagation that has the side effect of a Denial-of-Service (DoS) attack.

This DoS attack not only disrupts the systems that the attack is trying to infect but also the local network of the compromised host. Depending on the number of infected

hosts in a network the amount of load generated by these devices could cause a local network disruption. This disruption will vary from a slow network to an unusable network as pipes fill and devices fail from the unexpected load. Services running on any infected system will likely be slowed, possibly blocking their legitimate usage.

Nimda is a more advanced attack than Code-Red because it can attack and infect systems in multiple ways, some of which are fairly new to the Internet community. For example, Nimda will infect users with certain e-mail clients without the user launching the infected attachment. By placing copies of itself in network shares, any other user attempting to browse the file with Window's Explorer preview option enabled will load the worm's executable. Once a system is infected, Nimda appends a JavaScript command to all locally stored HTML files that will later load the worm's executable on any remote system that views the HTML file without user intervention. More information on Nimda can be found at:

<http://www.cert.org/advisories/CA-2001-26.html>



Cisco Recommendations for Mitigating Nimda

Patch All Vulnerable Systems

The most effective manner in which to mitigate the Nimda is to patch all systems that are vulnerable. This should be the first step. This is difficult with uncontrolled user systems in the local network and even more troublesome if they are remotely connected to the network via a virtual private network (VPN) or remote access server (RAS). However, determining which devices are exploitable can be simplified by the use of security auditing tools that look for vulnerabilities in server systems. For local workstations, the PC's browser and e-mail client may need to be patched. The following links provide information regarding infection mitigation on Microsoft products:

- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-026.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp>

Many vendors' products install and use Microsoft IIS to provide Web access for remote management and reporting and these will also be vulnerable unless patched. Microsoft Outlook and Outlook express mail applications that have the automatic execution of embedded MIME types vulnerability should also be patched. Versions of Microsoft Internet Explorer that contain the exploit should also be patched. Refer to the above URLs for vulnerable versions of these applications. If it is not possible to patch all systems in a timely manner consider deploying the technologies discussed in the following section for immediate mitigation benefit. You should also consider using these technologies proactively to mitigate future attacks by Nimda or other attacks altogether.

The second step in Nimda mitigation is to update all virus scanning software with the latest virus lists. As a good practice, run local scans on systems in case they were already infected. The final step would be to determine which devices in your network are still infected or vulnerable in case they were missed during the patching and virus scanning. These tasks can be carried out in part with network scanners, but primarily by analyzing alarms received from an Intrusion Detection System (IDS).

Security Technologies

This section discusses the technologies available in the Cisco Systems product line to mitigate Nimda and other attacks. To learn more about any of these technologies, or for Nimda mitigating configurations, refer to the SAFE white papers located at:

<http://www.cisco.com/go/safe>

Host-Based Intrusion Detection System

Host-Based Intrusion Detection System (HIDS) operates by detecting attacks occurring on a host on which it is installed. It works by intercepting OS and application calls, securing the OS and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity. It has two modes of operation: monitor (alarm only) and enforce. HIDS performs many security functions:

- Analyzes incoming HTTP traffic and via the use of generic rules and known attack signatures, determines if it is an attack.
- Analyzes the HTTP server's actions to determine if they reflect its normal mode of operations.
- General OS protection including buffer overflow prevention and binary modification.



When the worm attempts to compromise a HIDS protected Web server, the attack will fail and the server will not be compromised. HIDS blocks the worm-like infection methods (spreading via Microsoft IIS vulnerabilities) by locking down the Web server. HIDS also prevents Directory Traversal and remote code execution attacks as well as unauthorized changes to Web content thus limiting the capability of the worm to alter Web pages in order to spread itself to other servers. Finally, HIDS will prevent the Web server from being compromised via HTTP and IIS exploits through attack signature detection.

The following HIDS rules will prevent Nimda from succeeding:

- IIS Directory Traversal
- IIS Directory Traversal and Code Execution
- IIS Double Hex Encoding Directory Traversal

NOTE: The virus-like, manual infection methods, such as opening an e-mail attachment, manually executing an infected file, browsing to an infected Web site, are not blocked by HIDS. These can be mitigated by the security best practices covered in SAFE, including virus scanning, and through education of the user base. For instance, administrators should not run client e-mail applications or browse the Web on production Web servers. It is also a best practice not to run network shares on public servers.

It may appear that deploying HIDS has the same problem with exploitation mitigation as discussed previously for applying system patches. However, HIDS clients are significantly easier and less obtrusive to install on running systems, and they are less likely to require system interruptions or reboots. To target specific systems for HIDS installation for the current problem, use a network security scanner to identify those systems that are running Web services. To mitigate future attacks beyond Nimda consider installing HIDS on critical servers.

Network-Based Intrusion Detection System

Network-Based Intrusion Detection System (NIDS) operates by first detecting an attack occurring at the network level and then either takes a corrective action itself or notifies a management system where an administrator can take action. Attacks are discovered by looking for their signatures in traffic flows in the network. Attack detection triggers NIDS to send an alarm and then take a pre-configured action. The two possible actions are shunning and TCP resets. Since NIDS is not in the data path, meaning it receives a copy of a packet as it traverses through the network verses routing the packet, NIDS cannot filter the first packet in an attack. Subsequent packets can be filtered via a feature known as shunning that modifies the upstream access-control device to block any further access from the IP address of the attacking system. TCP resets attempt to tear down the TCP connection by sending a fabricated reset that appears to be from the receiving device to the attacking device. NIDS identifies many of the Web application attacks used by Nimda worm and provides details about the affected and compromised hosts.

The following Cisco IDS Network Sensor alarms will fire:

- WWW WinNT cmd.exe Access (SigID 5081)
- IIS CGI Double Decode (SigID 5124)
- WWW IIS Unicode Attack (SigID 5114)
- IIS Dot Dot Execute Attack (SigID 3215)
- IIS Dot Dot Crash Attack (SigID 3216)



NIDS operators will not see an alarm that identifies Nimda by name. They will see a series of these alarms as Nimda tries different exploits to compromise the target. These alarms will identify the source address of hosts that have been compromised and should be isolated from the network, cleaned, and patched.

Virus Scanning

Virus scanning software provides real-time host attack mitigation against malicious code and viruses. As with Nimda, viruses may have multiple paths into the system including e-mail, browsing, file exchange, and so on. These multiple paths may themselves intrinsically provide multiple vectors into the system. Web pages for instance may use ActiveX, Java, and JavaScript to load remotely available code in order to provide additional functionality. However all of these mechanisms are entry points for executing malicious code on the system. In most cases, the user is prompted as to whether they will allow the remote code to execute. Due to a lack of user education, most will click “yes” without hesitation. Worse yet, older Web browsers will not even prompt the user and execute the code automatically. In order for virus scanning to be successful, the following should be completed at regular intervals:

- Routine host local file scanning
- Routine virus-list/signature updating
- Routine monitoring of alerts generated by the host scanners

A list of Cisco partners that provide virus scanning software is listed at the end of this document.

Access Control

Stateful firewalling—provides a number of security features to proactively mitigate Nimda. First, the stateful inspection engine can control connection attempts at a level more granular than normal by validating proper protocol adherence. This filtering could be used to allow only inbound connections to a Web server and at the same time disallow that Web server to initiate outbound connections thus limiting the worms’ ability to self-propagate. This is particularly applicable for DMZ Web server deployments. As discussed in SAFE, your Web servers don’t normally need the ability establish outbound connections to say, surf the Web. In most cases they only need to respond to incoming Web requests. Second, it has the capability of limiting the number of permitted inbound connections to a server so that the server will not become overwhelmed. In the case of Nimda this will block excessive inbound exploitation connection attempts once the maximum allowed number are reached.

Ingress filtering—is typically carried out by access-control on the perimeter of the network. It is used to block access to hosts and services that should not be publicly available. For instance, it is a security best practice to disallow incoming connection requests to hosts or networking devices unless those hosts or devices are actively participating in providing a publicly accessible service. As it pertains to Nimda, incoming HTTP connections would be blocked from accessing any possibly exploitable user systems or non-publicly available Web servers. These same filters, however, would need to allow access to a publicly available Web presence or E-commerce server. Ideally, the public servers are under tight administrative control and have the latest patches. Ingress filtering would in effect block Nimda exploitation attempts targeted at user systems.

Egress filtering—is also typically carried out by access-control on the perimeter of the network. This filtering blocks a local host’s access outbound out of your network. Devices that do not need outbound Internet access, such as the majority of the networking devices in your network or Web servers that only serve the internal environment, should not be allowed to initiate outbound connections. As this pertains to Nimda, if a device is compromised it will not be able to infect an external network since the traffic will be intercepted and dropped at the perimeter of your network. Additional layers of egress filtering in the network besides at the WAN edge could also be used to disallow an infected



public Web server (or its entire segment for the case of a Web farm) from infecting private internal servers that were protected by the edge ingress filtering. For more information on access control and filtering please refer to the SAFE white papers.

Private VLANs

Private VLANs work by limiting which ports within a VLAN can communicate with other ports in the same VLAN. Typically, private VLANs are deployed so that the hosts on a given segment can only communicate with their default gateway and not the other hosts on the network. For instance, should a Web server be compromised by Nimda, it will not be able to initiate infection attempts to other Web servers in the same VLAN even though they exist in the same network segment. This access control is carried out by assigning hosts to either an isolated port or a community port and is an effective way to mitigate the effects of a single compromised host. Isolated ports can only communicate with promiscuous ports (typically the router). Community ports can communicate with the promiscuous port and other ports in the same community.

For more information on private VLANs, refer to:

<http://www.cisco.com/warp/public/473/90.shtml>

The SAFE Blueprint

The SAFE blueprint utilizes many security technologies to mitigate Nimda. For this reason, the SAFE blueprint is “Nimda safe.” Ingress and egress filtering is not only applied at the network edge but also between virtually all SAFE modules. This filtering restricts outbound access from infected servers and inbound infection attempts against user systems. Stateful firewalling protects both the user and server segments in addition to the filtering and provides DDOS connection rate limiting for the public servers. NIDS is deployed not only in all public segments to identify Nimda infection attempts but also behind the network edge filtering and stateful inspection to determine if any exploitation attempts made it through the edge. HIDS is installed on all publicly available servers and even critical internal servers that do not have Internet access to guard against possible infection from uncontrolled user systems. Private VLANs are deployed in public service segments where multiple public servers are available to guard against trust exploitation.

Conclusion

The technologies discussed in this document not only mitigate the potential damage done by Nimda and its variants but also virtually any attack. It is important to remember that security has its place throughout the infrastructure and the discussed technologies prove this. Protecting your network and its resources against Nimda is only the first step. It is necessary to be proactive when it comes to security so that you can not only protect the network against Nimda but future attacks as well. Establishing a security policy, implementing some of the discussed features, and regular in-house or outsourced posture assessments will secure your network and keep it secure.

This document has addressed a small sampling of the documented security and network design best practices available from Cisco Systems. For additional information on securing your network, refer to the SAFE blueprint at: www.cisco.com/go/safe

As with any feature, if you are considering enabling some of the discussed features, ensure your devices have sufficient CPU resources available. Also realize though that the increased load brought on by enabling these features is significantly less than that of the load brought on by an internal Nimda infection.

As a special note, the SAFE blueprint was released in October of 2000. No design or implementation modifications were required to deal with the Code-Red or Nimda attacks. Only NIDS signature and virus list updates at regular intervals were necessary to detect the new exploits and attacks. As Nimda, Code-Red, and other high-profile network exploits constantly remind us, designing network security in a reactive manner is not recommended. Only by taking a comprehensive approach to network security founded on good security policy decisions, can your organization be assured that the risks you are taking are known, and that virtually any potential threat can be effectively contained.

Links to Additional Information

CERT information on Nimda:

<http://www.cert.org/advisories/CA-2001-26.html>

The SAFE Blueprint:

www.cisco.com/go/safe

Cisco Information on Code-Red:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/scdam_wp.htm

Links to Cisco Products and Services

Cisco NIDS and HIDS:

<http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml>

Virus Scanning:

http://www.cisco.com/pcgi-bin/ecoa/displayProfile?PARTNER_ID=602

http://www.cisco.com/pcgi-bin/ecoa/displayProfile?PARTNER_ID=1003

Network Scanners:

<http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/index.shtml>

General Information on Cisco Security Products

Network Security:

<http://www.cisco.com/go/security>

Cisco Security Consulting:

<http://www.cisco.com/go/securityconsulting>

Cisco PIX Firewall:

<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R) BU/LW4784 06/03