

SAFE SQL Slammer Worm Attack Mitigation

Introduction

This document discusses the recently released SQL Slammer worm and its effects on the network and its hosts. Today numerous technologies are available for use in Cisco products that mitigate the detrimental effects of the worm. These include not only security technologies such as intrusion detection and packet filtering, but also virtual LAN (VLAN) segmentation, packet classification, and content services. In addition to these technologies the SAFE blueprint from Cisco combines security best practices and secure network design to mitigate worms and viruses like SQL Slammer and other network attacks. This paper contains much of the same information discussed in the Code-Red and Nimda white papers posted at www.cisco.com/go/safe. This is important to note because the core mitigation techniques stay the same as new worms are released.

SQL Slammer Background and Function

On Friday evening of January 24, 2003 a new worm was released onto the Internet and infected up to 35,000 hosts within a very short timeframe.

Because of the speed and the nature of the worm it has the capability of causing a denial of service to target networks. Several ISPs and enterprises noted significant link saturation due to the large volume of traffic caused by the worm. This traffic was

further amplified because of ICMP unreachable messages returned by routers for nonexistent hosts.

The SQL Slammer worm apparently does not contain malicious payload beyond the buffer overflow to gain access to the host running the SQL Server Resolution Service and then to set up the worm. Multiple instances of the worm can infect a host because the worm does not check for previous infections of the target system.

Cisco Recommendations for Mitigating SQL Slammer

The SQL Slammer worm has been identified and analyzed by several groups, including analysts from eEye Digital Security. Their analysis can be found at:

<http://www.eeye.com/html/Research/Flash/AL20030125.html>.

This worm appears to be based on the Microsoft SQL Server 2000 exploit noted in July 2002 by David Litchfield of Next Generation Security Software, Inc. This vulnerability is centered in the Microsoft SQL Server Resolution Service running on UDP port 1434 of SQL Server 2000 systems and systems with the Microsoft Desktop Engine 2000 (MSDE) installed. The worm sends multiple 376-byte packets to randomly-generated IP addresses. This particular worm does not appear to have a purpose beyond simply propagating itself; however, due to the nature of how it propagates it has caused significant problems for some service provider and enterprise networks.



The most effective method to contain this worm is the application of ingress and egress filters or access control lists (ACLs) blocking port 1434 UDP.

Ingress filtering is typically performed 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.

Pertaining to SQL Slammer, incoming SQL connections would be blocked from accessing any possibly exploitable user systems or non-publicly available SQL servers. These same filters, however, would need to allow access to a publicly available SQL 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 SQL Slammer exploitation attempts targeted at user systems.

Egress filtering is also typically performed by access control on the perimeter of the network. This filtering blocks a local host's access outbound from the network. Devices that don't need outbound Internet access, such as most of the networking devices in the network or SQL servers that serve only the internal environment, should not be allowed to initiate outbound connections.

As this pertains to SQL Slammer, if a device is compromised it will not be able to launch a DDoS attack against an external network because the traffic will be intercepted and dropped at the perimeter of the network. This setup will also guard against the DDoS attack flooding the Internet link and interfering with legitimate inbound or outbound traffic. Additional layers of egress filtering in the network in addition to those at the WAN edge could also be used to disallow an infected public SQL server (or its entire segment for the case of an SQL farm) from infecting private internal servers that were protected by the edge ingress filtering. For more information about access control and filtering, see the SAFE Blueprint white papers.

A sample ingress and egress filter rule to add to existing ACLs is provided in the configuration section at the end of this paper.

After further worm infection has been prevented through the use of ingress and egress filters, the next step is identifying and tracking vulnerable hosts as well as systems that may already be infected.

The first and most effective manner in which to mitigate the SQL Slammer worm is to patch all systems that are vulnerable. This patching 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. However, determining which systems are exploitable can be simplified by the use of security auditing tools that look for vulnerabilities such as the ones listed at the end of this paper.

Scanning for systems that may be running the Microsoft SQL Resolution Service provides for quick identification of potentially vulnerable hosts. After these vulnerable systems are identified they can be patched to remove the vulnerability. Monitoring log files for hits on the ACLs discussed above can identify hosts already infected by the SQL Slammer worm. The following links provide information about infection mitigation on Microsoft SQL products:

- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp>
- <http://www.microsoft.com/technet/security/virus/alerts/slammer.asp>



Future worms

The SQL Slammer worm is the third worm to appreciably affect the Internet in the past two years. Some of the more significant factors that allowed for the quick propagation and infection of this worm include:

- The slow application of the patch provided by Microsoft for the SQL Server Resolution Service
- Improper placement of database servers in networks
- Insufficient filtering

It is inevitable that another worm of similar magnitude will strike the Internet within the foreseeable future. Given that fact it is prudent for network engineers as well as management to take the necessary steps to protect their networks to the greatest extent possible. These steps can include some, if not all, of the technologies discussed in this paper. The SAFE Blueprint provides enterprises and service providers with a starting point with which to build secure, resilient networks.

If, given a newly discovered vulnerability in a service, it is not possible to patch all systems in a timely manner, consider deploying the technologies discussed in the following section. Consider using these technologies proactively to mitigate future attacks by variants of SQL Slammer or other attacks.

Security Technologies

This section discusses the technologies available in products from Cisco and other companies to mitigate SQL Slammer and other attacks. To learn more about any of these technologies, or for SQL Slammer mitigating configurations, see the SAFE Blueprint white papers at <http://www.cisco.com/go/safe>.

End-Point Intrusion Prevention System

The Okena Corporation's (www.okena.com) end-point intrusion prevention system (EPIPS) operates by detecting attacks that occur on a host on which it is installed. It works by intercepting application resource requests to the operating system to make a real-time allow/deny decision according to the defined application security policy. The EPIPS responds based upon which system it is installed on:

- On the EPIPS Management Console (running MSDE), the EPIPS Default Manager policy prevents incoming connections to the MSDE on the SQL port.
- On a Microsoft SQL server 2000 system, the EPIPS default policy is designed to accept incoming connections to SQL; however, the EPIPS buffer overrun logic detects and terminates the Slammer worms attempt to invade the system.
- On a desktop system, the EPIPS Desktop policy prevents incoming connections to the MSDE on the SQL port.

In the case of the SQL Slammer worm the EPIPS prevents the initial buffer overrun that it exploits and the default policies provide additional protection at both the server and desktop level against the propagation of this worm and others like it.

It may appear that deploying EPIPS has the same problem with exploitation mitigation as discussed previously for applying system patches. However, EPIPS 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 EPIPS installation for the current problem, use a network security scanner to identify those systems that are running Web services. To mitigate future network attacks beyond SQL Slammer, consider installing EPIPS on critical servers.



Network-Based Intrusion Detection System

The network-based intrusion detection system (NIDS) operates by first detecting an attack occurring at the network level and then either taking a corrective action itself or notifying 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. Because NIDS is a passive monitoring mechanism in the data path (meaning it receives a copy of a packet as it traverses through the network versus routing the packet), NIDS cannot filter the first packet in an attack. Subsequent packets can be filtered via a feature known as shunning, which 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.

Refer to the SAFE Blueprint white papers before enabling shunning in a network for more information as well as special considerations when using this feature. Because the SQL Slammer attack is contained within a single packet, NIDS cannot stop the attack. NIDS does, however, provide visibility by sending an alarm when SQL Slammer attacks traverse the network. For more information about NIDS, see: <http://www.cisco.com/go/ids>.

Access Control

Stateful firewalling provides numerous security features to proactively mitigate the SQL Slammer worm. 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 SQL server and at the same time disallow that SQL server from initiating outbound connections, thus limiting the ability of the worm to self-propagate.

As discussed in the SAFE Blueprint, SQL servers do not normally need the ability to establish outbound connections to external systems. In most cases they need to respond only to incoming SQL requests. Second, stateful firewalling has the capability of limiting the number of permitted inbound connections to a server so that the server does not become overwhelmed. In the case of SQL Slammer, this limiting blocks inbound exploitation connection attempts.

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 communicate only with their default gateway and not the other hosts on the network. For instance, if the SQL Slammer worm compromises an SQL server, the SQL Slammer worm will not be able to initiate infection attempts to other SQL servers in the same VLAN even though they exist in the same network segment. This access control, carried out by assigning hosts to either an isolated port or a community port, is an effective way to mitigate the effects of a single compromised host. Isolated ports can communicate only with promiscuous ports (typically the router). Community ports can communicate with the promiscuous port and other ports in the same community.

For more information about private VLANs, refer to: <http://www.cisco.com/warp/public/473/90.shtml>



Additional Cisco Networking Technologies to Assist in Mitigating the SQL Slammer Worm

Network-Based Application Recognition

Network-based application recognition (NBAR) is a classification engine in Cisco IOS® Software that can recognize a wide variety of application-level protocols, including the Microsoft SQL protocol and protocols that use dynamic port assignments. After the traffic has been classified by NBAR, appropriate QoS policies can be applied to the traffic classes. NBAR can recognize the SQL Slammer worm. Unlike NIDS, NBAR can immediately classify the SQL Slammer traffic and drop the packet before it reaches the server. NBAR can be used inbound and outbound to mitigate the effects of the SQL Slammer worm.

For more information about NBAR, see:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e2/nbar2e.htm>

Sink-Hole Routers

Setting up a sink-hole router will assist in determining which systems in your environment are infected when NIDS is not available. This scenario works by using addresses not yet allocated by the Internet Assigned Numbers Authority (IANA) that the SQL Slammer worm will inadvertently attempt to exploit. The sink-hole router advertises these networks locally (only), and any attempts at reaching them are then routed to the router. When received, they can be logged and discarded. The results of the logs will provide a list of infected hosts.

For more information about how to configure this function, see: <http://www.cisco.com/public/cons/isp/security/>

Unicast Reverse Path Forwarding

The Unicast Reverse Path Checking (RPF) feature helps mitigate problems caused by the introduction of spoofed IP source addresses into a network. It works by discarding IP packets that lack a verifiable IP source address. There are two Unicast RPF checking modes:

- Strict checking mode, which verifies that the source IP address exists and is reachable through the input interface
- Exist-only checking mode, which only verifies that the source IP address exists in the Forwarding Information Base (FIB) table

Customers reported that the use of the command `ip unicast reverse path forwarding` did provide some appreciable measure of relief from the SQL Slammer worm.

NetFlow

NetFlow switching is a high-performance, network-layer switching path that can capture a wide range of traffic statistics including user, protocol, port, and type of service information. This information can be used to identify network traffic patterns and help network engineers respond to attacks such as the SQL Slammer worm.

For more information about how to configure NetFlow, see: http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800880f9.html



Committed Access Rate

Committed Access Rate (CAR) can be used to rate-limit traffic based on a set of criteria and provides for configurable actions such as transmit, drop, set precedence, or set QoS group when the traffic meets or exceeds the rate limit. These criteria include such metrics as incoming interface, IP precedence, QoS group, or IP access list criteria as well as others. CAR performs two QoS functions:

- Bandwidth management through rate-limiting
- Packet classification

By using CAR network engineers can classify and control traffic into and out of their networks, thereby providing a capability to prevent the bandwidth saturation seen by several service providers during the SQL Slammer worm propagation. For more information regarding CAR, see: http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800880f9.html

The SAFE Blueprint

The SAFE Blueprint uses all the security technologies listed above to mitigate the SQL Slammer worm. For this reason, the SAFE Blueprint is “SQL Slammer worm safe.” Ingress and egress filtering is applied not only at the network edge but also between virtually all SAFE Blueprint modules. This filtering restricts outbound access from infected servers and inbound infection attempts against user systems. Using firewalls 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 SQL Slammer worm infection attempts but also behind the network edge filtering. EPIPS 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 mitigate not only the potential damage the SQL Slammer worm can cause 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 a network and its resources against worms like SQL Slammer is only the first step. It is necessary to be proactive when it comes to security to protect a network not only against this worm but also future network attacks.

Establishing a security policy, implementing some of the discussed features, and regular in-house or outsourced posture assessments will secure a 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 about securing your network, see the SAFE Blueprint at www.cisco.com/go/safe.

As with any feature, ensure that all devices have sufficient CPU resources available before enabling any of the features discussed in this document. Also realize, however, that the increased load brought on by enabling these features is significantly less than the load brought on by an internal SQL Slammer worm infection.



As a special note, the SAFE Blueprint was released in October 2000. No design or implementation modifications were required to address SQL Slammer. Only NIDS signature updates at regular intervals were necessary to detect the SQL exploit and the SQL Slammer worm. This and other high-profile network exploits constantly provide reminders that designing network security reactively is not recommended. Only by taking a comprehensive approach to network security founded on good security policy decisions can an organization be assured that the risks taken are known, and that virtually any potential threat can be effectively contained.

Configuration Information

This section provides sample configurations for some of the technologies discussed in this document that were not tested for attack mitigation capabilities as part of SAFE Blueprint or that later required configuration changes. EPIPS is not discussed because the mitigation capability it provides is ready to use and requires no additional configuration beyond placing the system in active mode.

Cisco IOS ACLs

The Cisco IOS ACLs for mitigating the SQL Slammer worm are provided below. Care must be taken when considering whether to use the log-input argument to the access-list command. It is possible to substantially increase the CPU usage on the router because of the logging on the ACL. If router performance degrades due to the introduction of these ACLs, discontinue the logging on the first ACL.

```
access-list 101 deny udp any any eq 1434 log-input
access-list 101 permit ip any any
```

A more fine-tuned approach would be to create an ACL for the offending SQL Slammer worm traffic and then use a class-based policing to drop the packets at the ingress interface.

1. Create ACL

```
access-list 101 deny udp any any eq 1434
access-list 101 permit ip any any
```

2. Match on ACL and packet length

```
class-map match-all slammer_worm
match access-group 101
match packet length min 404 max 404
```

3. Use class-based policing to drop matching packets at the ingress interface

```
policy-map drop-slammer-worm
class slammer_worm
police 1000000 31250 31250 conform-action drop exceed-action drop violate-action drop
```



NIDS Attack Signatures

The signatures provided below were added to NIDS systems (Cisco Secure IDS 4210 Sensor, Cisco Secure IDS 4230 Sensor, Intrusion Detection System Module) in many modules of the SAFE Blueprint.

SQL Slammer Worm

String:

```
"\x04\x01\x01\x01\x01.*[.][Dd][Ll][Ll]"
```

Occurrences: 1

Port: 1434

Recommended alarm severity level:

- High (Cisco Secure Policy Manager [SPM])
- 5 (UNIX Director)

The latest NIDS signature database is available at the link below:

<ftp://ftp-eng.cisco.com/pub/titanium/IDS-sig-3.1-3-S39.bin>

NBAR

NBAR provides for the creation of a custom protocol to monitor traffic not normally associated with NBAR. Following is an example configuration:

Custom Protocol in NBAR

1. Create custom protocol

```
ip nbar port-map custom-01 udp 1434
```

2. Create class-map

```
class-map match-all slammer_worm
match protocol custom-01
match packet length min 404 max 404
```

3. Use class-based policing to drop the matching packets at the ingress interface

```
policy-map drop-slammer-worm
class slammer_worm
police 1000000 31250 31250 conform-action drop exceed-action drop violate-action drop
```



NetFlow

NetFlow can be configured and enabled on a variety of Cisco routers. The following configuration provides a general description of how to configure NetFlow. Consult the Cisco Web site (www.cisco.com) for more specific information about a particular router platform. To configure NetFlow on a NetFlow-capable router:

```
Router# config t
Router# (config) interface serial 0/1
Router#(config-if) ip route-cache flow
Router#(config-if) exit
Router#(config) exit
Router#
```

After NetFlow has been enabled on the router, the information can be exported to a variety of network management applications. To export NetFlow statistics:

```
Router# (config) ip flow-export 192.168.155.1 700
```

To view NetFlow statistics for port 1434:

```
Router# show ip cache flow | include 059A
```

CAR

Like NetFlow, committed access rate can be configured on a variety of Cisco routers. The following configuration is an example:

```
Router# (config) access-list 150 deny udp any any eq 1434
Router# (config) access-list 150 permit ip any any
Router# (config) interface fastEthernet 0/0
Router# (config-if) rate-limit input access-group rate-limit 150 8000 1500 20000 conform-action drop exceed-action drop
Router# (config-if) exit
Router# (config) exit
Router#
```

Links to Additional Information

Cisco Systems, Inc. response to the SQL Slammer worm:

http://www.cisco.com/en/US/products/hw/iad/ps497/products_security_advisory09186a0080133399.shtml

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_security_advisory09186a00801334af.shtml

NIDS signature ID for the SQL Slammer worm:

<http://www.cisco.com/go/csec>. Search for ID 4701.



EPIPS:

<http://www.okena.com>

http://www.okena.com/Areas/Solutions/solutions_attack_slammer.html

Microsoft response to the SQL Slammer worm and required patches:

<http://www.microsoft.com/technet/security/virus/alerts/slammer.asp>

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp>

eEye analysis of the SQL Slammer worm:

<http://www.eeye.com/html/Research/Flash/AL20030125.html>.

Computer Emergency Response Team (CERT) information about the SQL Slammer worm:

<http://www.cert.org/advisories/CA-2003-04.html>

Links to Cisco Products and Services

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

Information about Cisco security products and security consulting:

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

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

The 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. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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)