January 27, 2003 - UPDATE
Microsoft SQL Denial of Service Worm Notification Extreme Networks Solution

A new virus that takes advantage of a vulnerability in the Microsoft SQL server client/server communication process rapidly spread through the Internet starting on Saturday, January 25th around 12:30am PST. The virus (called by various names including “slammer”, “sapphire” or “SQ hell”), wreaks havoc on Microsoft SQL servers and the connected networks by sending out thousands of ICMP packets. The signature of this worm is high volumes of UDP traffic to port 1434.

Though the Denial of Service (DoS) attack is not targeting internetworking equipment, internetworking equipment may be affected. this includes Extreme Networks switches.

Symptoms:

The symptoms exhibited by Extreme Network switches affected by this attack include the following:

Extremely high "NetTask Utilization"

1. Log into Extreme Network switch
2. Perform "top"
3. NetTask Utilization over 50%

Show CLI Response
Slow response from typing commands

Frequent Switch reboots
Check the system log and check for frequent reboots

Other problems reported:

- the worm appears to randomly choose IP addresses to probe, and can scan into class D multicast address range.
- when the DoS attack would use Class D Internet addresses, the next-hop switch servicing multicast requests would indicate high CPU utilization as IGMP sender entries would be quickly populated into the multicast sender list. This could lead to system CPU resources being over-utilized, a high number of multicast entries in the IGMP snooping entry table, and the following message may also be seen in the system log where "tBGTask" is the task reporting the failure:

```
<WARN:HW> tBGTask: Reached maximum otp ExtraMC index allocation
```

Workarounds

Thus far the best mitigation is to block traffic destined to UDP port 1434. Care must be taken to minimize the impact on mission critical services 1434/udp that are legitimately used by Microsoft SQL Server. Once udp port 1434 is blocked, the spread of the worm in its current form will be contained. Infected systems will still be infected and able to spread within the contained section of the network, therefore it is strongly recommended that all affected servers be repaired according to the vendor recommendations. Other suggested workarounds are:

- Remove SQL Severs affected by this virus from the network and ensure the creation of an ACL to block ports 1434. This will block the attack but not fully address the effect on multicast entries by switches servicing the affected devices directly.
- Disable IGMP Snooping on the switch being affected. This will affect routing protocols using multicast addresses and multicast traffic on that switch.
- If possible, disable the port that services the infected server.

The unicast-based attack can be effectively stopped on Extreme switches via Access Control Lists. However, when multicast addresses are used, it is not completely filtered by the ACLs. This may cause degradation in switch performance as CPU and memory resources are impacted at the switch.

For Extreme 6.X Users

The temporary solution is to create an ACL in the Extreme Networks switch to block the DoS attack or to turn off the SQL servers. To block the DoS attack, create the following ACL:

```
create access-list block_1434 udp destination any ip-port 1434 source any ip-port any deny ports any precedence <number>
```

Where <number> is a low enough number to insure that other ACLs don't preempt this entry.

Note, the ACL will block the attack but not fully address the effect on multicast entries by switches servicing the affected devices directly.

Extreme Networks has released a patch that will protect the switches against both unicast and multicast traffic patterns.
The patch is based on the ExtremeWare 6.2.2 Code base and can be available by contacting Extreme TAC Support
via phone at 800 998 2408 or via email to Support@extremenetworks.com

For ExtremeWare 7.X Users

The customers running ExtremeWare 7.0.0 can protect themselves against this attack by disabling the IGMP Snooping on selected VLANS. This is in addition to the creation of the ACL rule for blocking UDP traffic to port 1434.

```
create access-list block_1434 udp destination any ip-port 1434 source any ip-port any deny ports any precedence <number>
```

Where <number> is a low enough number to insure that other ACLs don't preempt this entry.

IGMP Snooping has to be disabled on VLANS that are directly connected to the MS SQL Servers. ACL rule will block the unicast UDP traffic, where as disabling IGMP Snooping would stop the flooding of the multicast addresses, stabilizing the network. L3 Unicast Routing will continue to function with IGMP Snooping disabled. However, IP Multicast routing needs to be disabled on these vlans. If there are any multicast servers, they needs to be moved into separate vlans.

The commands to do this, which is a workaround in 7.0 only, is:

```
disable igmp snooping vlan <vlan name>
```

To change the snooping mode you must disable IP multicast forwarding. Use the command:

```
    disable ipmcforwarding vlan <vlan name>
```

auto-completion can be used or by pressing the tab key a list of vlans
is displayed for this parameter

Permanent resolution:

For Permanent resolution to stop this attack, the Microsoft SQL server needs to be upgraded.

Details on the Microsoft fix can be found at their website.
<http://www.microsoft.com/technet/security/bulletin/MS02-039.asp>

If you are having network difficulties, please contact regional TAC center: Corporate: 1-800-998-2408, EMEA: 31-30-800-5000; Japan: 81-3-5842-4020; APAC 1-800-988-2408.

Extreme Networks Technical Assistance Center