

## **W32.Welchia.Worm, W32/Nachi.worm, WORM\_MSBLAST.D, Lovsan.D**

There have been numerous reports of the W32.Welchia.Worm slowing down network performance. This worm exploits two Microsoft vulnerabilities: DCOM PRC using TCP port 135 and WebDav using TCP port 80.

Additional information on these vulnerabilities can be located at Microsoft's Security site:

[Microsoft Security Bulletin MS03-026](#)

[Microsoft Security Bulletin MS03-007](#)

Once a machine is infected with the W32.Welchia.Worm, it performs the following:

1. It attempts to download the DCOM RPC patch from Microsoft's Windows Update Web site. If it is successful, it will install the new DCOM RPC patch and reboot the infected computer.
2. It tries to infect other active Windows PCs by using the PING protocol (ICMP echo request). This will cause the amount of ICMP traffic to rise on infected networks and may decrease performance of the LAN, WAN, or Internet connections.
3. The ICMP packets used by this worm are 92 bytes in length and are ICMP type 8 (echo request) packets. The worm randomizes the destination IP Address in an attempt to spread itself as much as possible.
4. It attempts to remove the W32.Blaster.Worm

Many virus detection software companies have posted tools to detect and patch the infected or uninfected computers from this virus. For more information, please check out these vendors sites and search their sites using the search criteria of "Welchia" or "Nachi".

Microsoft's Site: <http://www.microsoft.com/security/antivirus/nachi.asp>

Symantec's Site: <http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>

### **Foundry Affected Systems:** BigIron, NetIron, FastIron, FWS4802

Once hosts are infected with the W32.Welchia.worm, ICMP Type 8 packets of 92 bytes will be used throughout the network to find new victim hosts. Based on Foundry's CAM based architecture, this will cause many new cache entries to be created in the switch and may deplete memory resources and degrade performance. Symptoms exhibited can include, but not limited to:

- High CPU utilization
- Large IP cache tables
- Depletion of memory resources
- Slow network performance
- Packet drops

### **Protective and Diagnostic Measures**

Once your computers are infected, the network load may increase with ICMP traffic to the point where connectivity is partially or fully disrupted. Steps that you can take to decrease the amount of ICMP on your networks until the Microsoft patch can be applied are:

1. Block inbound ICMP at each router port with an ACL. This will prevent the ICMP's from flooding the network backbone and allow you to gain control of your network bandwidth. Once control has been established, you can apply the patches one subnet at a time to remove the virus and prevent the computers from being re-infected.
2. Implement the ICPM Burst Maximum feature on your switches. For Layer 3 switches, when implemented at the global level, this command will protect the IP Address programmed on the router

interfaces. To prevent the ICMP flooding from traversing the L3 port, implement this command at the Layer 3 port level. For Layer 2 switches, implementing the ICMP Burst Maximum command at the global level will protect all interfaces and all ICMP packets traversing the switch will be calculated for the entire switch using the Burst Maximum value. The CPU will block any ICMP packets above the set threshold.

3. Look at the logs on your firewall, intrusion detection system, intrusion prevention system, or routers/switches to see which computers are the source of the ICMP floods. You can also place a sniffer on each router port or switch uplink to locate these infected PCs. This will give you an idea of which PCs are infected so you can patch them quickly.
4. Use the "dm raw" command to isolate infected hosts that are flooding the network with ICMP. If the output is 106 bytes in length for the majority of packets being forwarded to the CPU, then the worm is active on your network. An example of how to use the DM RAW feature to analyze ICMP packets:

dm raw normal	Turns on DM RAW in Brief Mode
dm raw max 100	Tells the debugger to stop after 100 records
dm raw filter 1 protocol icmp	Instructs the debugger to filter on ICMP packets
dm raw	Starts the debugger

5. For sFlow customers, look at the ICMP statistics for all monitored switches. The reports will show the offending infected hosts by showing the high amounts of transmitted ICMP packets. InMon customers can use the "Fan Out" reports to track ICMP.
6. Implement the latest patch from Foundry Networks and turn on the new ICMP ACL to block ICMP traffic based on packet size. This feature is included in the following revisions of Foundry software: version 7.7, version 7.6.0.4e, and version 7.5.0.5t. An examples of how to use the new ICMP ACL:

```
access-list 120 deny icmp any any any ip-pkt-len 92
access-list 120 permit ip any any
```

Apply this access-list inbound to the proper interface. Use the "show ip acl-traffic" command to see the number of ICMP packets being filtered by the ICMP ACL.

For more information on obtaining the latest Foundry Patches, visit the Technical Support web site on the Foundry Networks site at [www.foundrynet.com](http://www.foundrynet.com), call Foundry's TAC Center, or contact your Sales and SE team.