



Product Bulletin No. 362881

## Cisco Security Agent and the Microsoft MS06-035 Security Bulletin: Vulnerability in Server Service Could Allow Remote Code Execution

### SUMMARY

A critical vulnerability was announced on July 11, 2006, for Microsoft Windows 2000, Windows XP and XP Professional, and Windows 2003 Server operating systems (<http://www.microsoft.com/technet/security/Bulletin/MS06-035.mspx>). There is a remote code execution vulnerability in the Server service driver (SRV.SYS) that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. Microsoft has released patch updates for these vulnerable operating systems, available from its Website ([www.microsoft.com](http://www.microsoft.com)).

Cisco Systems® has obtained exploit files and has confirmed that Cisco® Security Agent is effective in stopping these exploits using the default security policy configuration. Current supported versions of Cisco Security Agent 4.03.x, 4.5.1.x, 5.0.0.x, and 5.1.0.x are effective in stopping the exploits seen to date.

### DETAILS OF THE VULNERABILITY

The first vulnerability is a buffer overflow vulnerability in the Microsoft mailslot server service that may allow a remote attacker to execute arbitrary code on vulnerable installations of the Microsoft Windows operating system. A mailslot is a temporary mechanism that uses TCP or UDP to facilitate data transfer between hosts. Buffer overflow can occur during the processing of mailslot messages. Authentication is not required to exploit this vulnerability, and code execution occurs within the context of the kernel. The Microsoft advisory states that attempts to exploit this vulnerability will most probably result in a denial-of-service condition caused by an unexpected restart of the affected system.

The second vulnerability is due to an uninitialized buffer in the server protocol driver, which could be exploited by attackers to remotely read fragments of memory used to store server message block traffic during transport.

### HOW CISCO SECURITY AGENT STOPS THE EXPLOIT

The default policies in Cisco Security Agent include a buffer overflow prevention rule that stops the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection.

The following actions have been observed being blocked by Cisco Security Agent running the default security policies:

- Execution of a system function from a buffer, through a buffer overflow

This testing is shown in Figure 1.

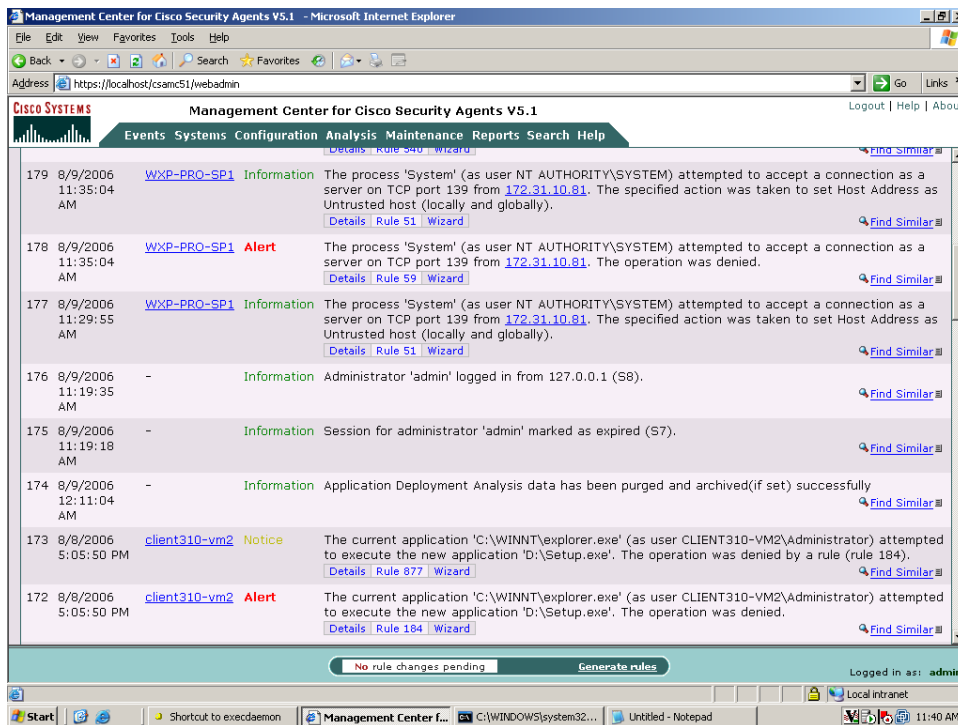
The exploit was tested at Cisco with the agent in Protect mode, which blocks malicious behavior. When the agent is in Protect mode (the typical operational configuration), the first rule would kill the exploit. No subsequent events would be seen, as the exploit would be terminated before it could perform any malicious actions.

Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for Cisco Security Agents to be effective. In short, this was a true test of “day zero” protection. This is similar to what Cisco has seen with earlier exploits and worms—the default Cisco Security Agent configuration stopped the exploit, with no binary or policy updates required. The following is a partial list of prior worms and exploits that Cisco Security Agent has stopped with the default security policy settings:

Bagle	E-mail worm	SQL Snake	Network worm
Blaster	Network worm	JPEG/GDI+	Malware downloader
Bugbear	E-mail worm	MyDoom	E-mail worm
Code Red	Network worm	Nimda	Network worm
Debploit	Network worm	Pentagone/Gonner	E-mail worm
Fizzer	E-mail worm	Sasser	Network worm
Gator/Gain	Spyware	Sircam	E-mail worm
Hotbar	Spyware	Sobig	E-mail worm
SQL Slammer	Network worm	Zotob	Network worm

This exploit is only the latest example of new and mutating attacks that can seriously impact an organization's computing and network environments. The key to preventing damage from these new attacks is the ability to stop an attack without requiring any changes to default configuration, along with multiple rules in the default policies that provide a defense in depth.

**Figure 1.** Cisco Security Agent Default Configuration Stops the Microsoft MS06-035 Exploit Tested on Cisco Security Agent 5.1





**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.  
168 Robinson Road  
#28-01 Capital Tower  
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.com Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Printed in USA

C25-362881-00 08/06