



November 16, 2006

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2006-11-16

Vulnerabilities in Client Service for NetWare

CVE-2006-4688, CVE-2006-4689

- **Synopsis**

The Client Service for NetWare (CSNW) allows a Windows client to access NetWare file, print, and directory services.

Successful exploitation could lead to execution of arbitrary code or cause the affected system to stop responding.

- **Vulnerable System or Application**

Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP Service Pack 2

Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

- **Vulnerability Information**

CVE-2006-4688

A boundary error in Client Service for Netware (CSNW) can be exploited to cause a buffer overflow via a specially crafted network message sent to the system. Successful exploitation allows execution of arbitrary code and an attacker could remotely take complete control of the affected system.

CVE-2006-4689

A denial of service vulnerability exists in Client Service for NetWare (CSNW) that could allow an attacker to send a specially crafted network message to an affected system running the Client Service for NetWare service. An attacker could cause the system to stop responding and automatically restart thus causing the affected system to stop accepting requests.

- **Resolution**

Microsoft has included fixes for the Client Service for Netware (CSNW) issues in the November 2006 Security Bulletin MS06-066 for affected Windows platforms.

- **Credits**

These vulnerabilities were discovered by Sam Arun Raj of McAfee Avert Labs.

- **Legal Notice**

Copyright (C) 2006 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.