

Cisco Security Response: Mitigating Exploitation of the MS06-040 Service Buffer Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-08/msg00305.html>

- *From:* "Paul Guibord" <pguibord@xxxxxxxxxxxx>
 - *Date:* Wed, 16 Aug 2006 09:06:08 -0400
-

First off I hope this is the proper place to discuss this. Please read the Security response from Cisco below. We have SSL VPN (SVC, Tunneling) remote users that establish sessions with our corporate network. They need the ability to map drives to servers once the session is established. In order to map drives it requires that TCP ports 139 and 445 to be open and there in lies the problem so I cannot filter these ports. Cisco's ASA Secure Desktop allows me to check for the presence of service packs and any registry entry on the remote client PC's and can restrict access if they are not installed. I believe that Microsoft released a fix for this vulnerability last week and would like to ensure that our remote users have the fix applied and if not deny access. Can anyone provide the necessary registry entry that I am to look for to ensure they have it installed before allowing them to establish a session.

Thanks,

Paul

http://www.cisco.com/en/US/products/ps6120/tsd_products_security_respons_e09186a008070c75a.html

Cisco Response

Vulnerability Characteristics

Attack Type: Unauthenticated, Remote, No interaction

Vulnerability Impact: Ability to perform remote code execution with the privileges of SYSTEM or create a Denial of Service

Attack Vector: Network Traffic on TCP ports 139 and 445

CVE ID: 2006-3439

Vulnerability Overview

This document contains information to assist Cisco customers in mitigating attempts to exploit the Microsoft Server Service Buffer Overflow Vulnerability. There is a remote code execution vulnerability in Server Service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected

Cisco Security Response: Mitigating Exploitation of the MS06-040 Service Buffer Vulnerability

system.

Computers using the following operating systems are affected:

Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP Service Pack 1

Microsoft Windows XP Service Pack 2

Microsoft Windows XP Professional x64 Edition

Microsoft Windows Server 2003

Microsoft Windows Server 2003 Service Pack 1

Microsoft Windows Server 2003 for Itanium-based Systems

Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

Microsoft Windows Server 2003 x64 Edition

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

http://www.cenzic.com/products_services/download_hailstorm.php
