

ZDI-07-055: Microsoft Windows DCERPC Authentication Denial of Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-10/msg00152.html>

- *From:* zdi-disclosures@xxxxxxxxx
 - *Date:* Wed, 10 Oct 2007 14:51:32 -0700
-

ZDI-07-055: Microsoft Windows DCERPC Authentication Denial of Service Vulnerability

<http://www.zerodayinitiative.com/advisories/ZDI-07-055.html>

October 10, 2007

-- CVE ID:
CVE-2007-2228

-- Affected Vendor:
Microsoft

-- Affected Products:
Windows 2000 SP4
Windows XP SP2
Windows 2003 SP1
Windows Vista

-- TippingPoint(TM) IPS Customer Protection:
TippingPoint IPS customers have been protected against this vulnerability since October 9, 2007 by Digital Vaccine protection filter ID 5657. For further product information on the TippingPoint IPS:

<http://www.tippingpoint.com>

-- Vulnerability Details:
This vulnerability allows remote attackers to crash systems with vulnerable installations of the Microsoft Windows operating system. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the RPC runtime library rpcrt4.dll during the parsing of RPC-level authentication messages. When parsing packets with the authentication type of NTLMSSP and the authentication level of PACKET, an invalid memory dereference can occur if the verification trailer signature is initialized to 0 as opposed to the standard NTLM signature. Successful exploitation crashes the RPC service and subsequently the entire operating system.

-- Vendor Response:

ZDI-07-055: Microsoft Windows DCERPC Authentication Denial of Service Vulnerability

Microsoft has issued an update to correct this vulnerability. More details can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms07-058.msp>

— Disclosure Timeline:

2007.02.05 – Vulnerability reported to vendor

2007.10.09 – Digital Vaccine released to TippingPoint customers

2007.10.10 – Coordinated public release of advisory

— Credit:

This vulnerability was discovered by Tenable Network Security.

— About the Zero Day Initiative (ZDI):

Established by TippingPoint, a division of 3Com, The Zero Day Initiative (ZDI) represents a best-of-breed model for rewarding security researchers for responsibly disclosing discovered vulnerabilities.

Researchers interested in getting paid for their security research through the ZDI can find more information and sign-up at: