

[NT] Microsoft Windows DCERPC Authentication Denial of Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 11 Oct 2007 15:28:54 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Microsoft Windows DCERPC Authentication Denial of Service Vulnerability

SUMMARY

A vulnerability allows remote attackers to crash systems with vulnerable installations of the Microsoft Windows operating system. Authentication is not required to exploit this vulnerability.

DETAILS

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:

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

[NT] Microsoft Windows DCERPC Authentication Denial of Service Vulnerability

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

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2228>>
CVE-2007-2228

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>
The Zero Day Initiative (ZDI).
The original article can be found at:
<<http://www.zerodayinitiative.com/advisories/ZDI-07-055.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-055.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.