

[UNIX] Multiple Vendor rdesktop Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-05/msg00005.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 9 May 2008 15:15:22 +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>

Multiple Vendor rdesktop Vulnerabilities

SUMMARY

<<http://www.rdesktop.org/>> rdesktop is "an open source client that speaks the Remote Desktop Protocol (RDP). This allows Unix-based users to login to Windows Terminal Servers". Multiple vulnerabilities have been found in the rdesktop client, these vulnerabilities could be used to cause the program to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * rdesktop version 1.5.0

Multiple Vendor rdesktop channel_process() Integer Signedness Vulnerability

Remote exploitation of an integer signedness vulnerability in rdesktop, as included in various vendors' operating system distributions, allows attackers to execute arbitrary code with the privileges of the logged-in user.

The vulnerability exists within the code responsible for reallocating dynamic buffers. The rdesktop xrealloc() function uses a signed comparison

[UNIX] Multiple Vendor rdesktop Vulnerabilities

to determine if the requested allocation size is less than 1. When this occurs, the function will incorrectly set the allocation size to be 1. This results in an improperly sized heap buffer being allocated, which can later be overflowed.

Analysis:

Exploitation of this vulnerability results in the execution of arbitrary code with the privileges of the logged in user. In order to exploit this vulnerability, an attacker must persuade a targeted user to connect to a malicious RDP server.

Vendor response:

The rdesktop maintainer has addressed this vulnerability with CVS revision 1.162 of rdesktop.c. For more information, visit the following URL.

<http://rdesktop.cvs.sourceforge.net/rdesktop/rdesktop/rdesktop.c?view=diff&pathrev=HEAD&r1=text&tr1=1.162&r2=>
<http://rdesktop.cvs.sourceforge.net/rdesktop/rdesktop/rdesktop.c?view=diff&pathrev=HEAD&r1=text&tr1=1.162&r2=>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1803>
CVE-2008-1803

Multiple Vendor rdesktop process_redirect_pdu() BSS Overflow Vulnerability

Remote exploitation of a BSS overflow vulnerability in rdesktop, as included in various vendors' operating system distributions, allows attackers to execute arbitrary code with the privileges of the logged-in user.

The vulnerability exists within the code responsible for reading in an RDP redirect request. This request is used to redirect an RDP connection from one server to another. When parsing the redirect request, the rdesktop client reads several 32-bit integers from the request packet. These integers are then used to control the number of bytes read into statically allocated buffers. This results in several buffers located in the BSS section being overflowed, which can lead to the execution of arbitrary code.

Analysis:

Exploitation of this vulnerability results in the execution of arbitrary code with the privileges of the logged in user. In order to exploit this vulnerability, an attacker must persuade a targeted user to connect to a malicious RDP server.

Vendor response:

The rdesktop maintainer has addressed this vulnerability with CVS revision 1.102 of rdp.c. For more information, visit the following URL.

<http://rdesktop.cvs.sourceforge.net/rdesktop/rdesktop/rdp.c?annotate=1.102&pathrev=HEAD#11337>
<http://rdesktop.cvs.sourceforge.net/rdesktop/rdesktop/rdp.c?annotate=1.102&pathrev=HEAD#11337>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1802>

[UNIX] Multiple Vendor rdesktop Vulnerabilities

CVE-2008-1802

Multiple Vendor rdesktop iso_recv_msg() Integer Underflow Vulnerability
Remote exploitation of an integer underflow vulnerability in rdesktop, as included in various vendors' operating system distributions, allows attackers to execute arbitrary code with the privileges of the logged-in user.

The vulnerability exists within the code responsible for reading in an RDP request. When reading a request, a 16-bit integer value that represents the number of bytes that follow is taken from the packet. This value is then decremented by 4, and used to calculate how many bytes to read into a heap buffer. The subtraction operation can underflow, which will then lead to the heap buffer being overflowed.

Analysis:

Exploitation of this vulnerability results in the execution of arbitrary code with the privileges of the logged in user. In order to exploit this vulnerability, an attacker must persuade a targeted user to connect to a malicious RDP server.

Vendor response:

The rdesktop maintainer has addressed this vulnerability with CVS revision 1.20 of iso.c. For more information, visit the following URL.

<http://rdesktop.cvs.sourceforge.net/rdesktop/rdesktop/iso.c?annotate=1.20&diff_format=h&pathrev=HEAD#1101>
http://rdesktop.cvs.sourceforge.net/rdesktop/rdesktop/iso.c?annotate=1.20&diff_format=h&pathrev=HEAD#1101

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1801>>
CVE-2008-1801

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idefense@xxxxxxxxxxxx>> iDefense Labs Security Advisories.

The original article can be found at:

<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=698>>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=698>,

<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=697>>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=697>

and

<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=696>>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=696>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

[UNIX] Multiple Vendor rdesktop Vulnerabilities

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.