

[UNIX] Multiple Vendor libwpd Multiple Buffer Overflow Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00039.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 19 Mar 2007 14:49:53 +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 libwpd Multiple Buffer Overflow Vulnerabilities

SUMMARY

<<http://libwpd.sourceforge.net/>> libwpd is a C++ library used to decode and encode word perfect documents. It is commonly used as a plug-in in word processing utilities such as Open Office and Abiword. For more information please visit the following URL.

Remote exploitation of multiple buffer overflow vulnerabilities in libwpd, as included in various vendors' operating system distributions, could allow an attacker to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * libwpd version 0.8.7.
- * Previous versions may also be affected.

Note: This library is used by applications such as Abiword, Kword, and Open Office.

One problem specifically exists in the WP6GeneralTextPacket::_readContents function. This function reads in a series of integer values and sums them.

[UNIX] Multiple Vendor libwpd Multiple Buffer Overflow Vulnerabilities

This sum is then used to allocate a block of memory from the heap. The function then copies data from the file into the buffer using each operand from the addition as the number of bytes to copy. The summing operation leads to an integer overflow, and the buffer can then be overflowed by the copy operations.

Two additional problems exist in the WP3TablesGroup::_readContents() and WP5DefinitionGroup_DefineTablesSubGroup::WP5DefinitionGroup_DefineTablesSubGroup() functions. These functions read an integer value from an attacker supplied file, and uses the value as a loop counter. In the loop a statically sized buffer is filled with arbitrary data from the file. This leads to an exploitable heap overflow.

Successful exploitation of these vulnerabilities requires an attacker to persuade a user into opening a specially crafted Wordperfect (WPD) document. If successful, the attacker could execute arbitrary code with the permissions of the victim.

Vendor Status:

The libwpd maintainers have addressed these vulnerabilities with the release of version 0.8.9.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2007-0002>>
CAN-2007-0002

Disclosure Timeline:

- * 01/11/2007 – Initial vendor notification
- * 01/12/2007 – Initial vendor response
- * 03/16/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=490>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=490>

=====

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@xxxxxxxxxxxxxxxx

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

=====

[UNIX] Multiple Vendor libwpd Multiple Buffer Overflow Vulnerabilities

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.