

[NEWS] NOD32 Antivirus DOC parsing Arbitrary Code Execution Advisory

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00049.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 Dec 2006 17:12:35 +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>

NOD32 Antivirus DOC parsing Arbitrary Code Execution Advisory

SUMMARY

Founded in "1992, ESET is a global provider of security software for enterprises and consumers. ESET's award-winning, antivirus software system, NOD32, provides real-time protection from known and unknown viruses, spyware, rootkits and other malware". Multiple vulnerabilities have been found in the file parsing engine of NOD32 antivirus.

DETAILS

Vulnerable Systems:

- * NOD32 Antivirus version 1.1742 and prior

Immune Systems:

- * NOD32 Antivirus version 1.1743

In detail, the following flaw was determined:

- Divide by Zero in .CHM file parsing.
- Heap Overflow through Integer Overflow in .DOC File Parsing

[NEWS] NOD32 Antivirus DOC parsing Arbitrary Code Execution Advisory

The .DOC problem can lead to remote arbitrary code execution if an attacker carefully crafts a file that exploits the aforementioned vulnerabilities. The vulnerabilities are present in NOD32 Antivirus software versions prior to the update v.1.1743.

Solution:

The vulnerabilities were reported on Aug 24 and an update has been issued on September 08 to solve these vulnerabilities through the regular update mechanism.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@xxxxxxxx>> n.runs AG.

The original article can be found at:

<<http://eset.com/support/updates.php?pageno=61>>
<http://eset.com/support/updates.php?pageno=61>

=====

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

=====
=====

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.