

[NT] BitDefender AV Packed PE File Parsing Engine Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00041.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2006 16:53:40 +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>

BitDefender AV Packed PE File Parsing Engine Heap Overflow

SUMMARY

BitDefenderT provides security solutions to satisfy the protection requirements of today's computing environment, delivering effective threat management to over 41 million home and corporate users in more than 200 countries.

BitDefender has garnered many awards, accolades and certifications since its inception in 2001. From the prestigious European IST Prize, to the #1 Best Buy ranking from PC World, and most recently, the PC World "Best 100 Products of 2006," the Company is enjoying worldwide recognition for its superior technology and product offering.

A remotely exploitable vulnerability has been found in the Packet PE file parsing engine.

DETAILS

A heap overflow through integer overflow in Packed PE file parsing exists in BitDefender, this problem can lead to remote arbitrary code execution if an attacker carefully crafts a file that exploits the aforementioned

[NT] BitDefender AV Packed PE File Parsing Engine Heap Overflow

vulnerability.

Solution:

The vulnerabilities were reported on August 28 and an update has been issued on August 29 to solve this vulnerability. The update has been delivered immediately to all BitDefender users through the regular automatic update mechanism, so no user action is required.

Vendor communication:

- 2006/08/24 – initial notification of BitDefender
- 2006/08/25 – BitDefender Response
- 2006/08/26 – PGP keys exchange
- 2006/08/28 – PoC files sent to BitDefender
- 2006/08/29 – BitDefender confirmed the bug and fixed it.
- 2006/08/30 – BitDefender released fixes through automatic update.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@xxxxxxxx>> nRuns Security.

The original article can be found at:

<<http://www.bitdefender.com/KB323-en--cevakrnl.xmd-vulnerability.html>>
<http://www.bitdefender.com/KB323-en--cevakrnl.xmd-vulnerability.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@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.