



# CVE-2006-6627

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2006-6627
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-12-18 11:28:00 UTC
<b>Updated</b>	2018-10-17 21:49:00 UTC
<b>Description</b>	Integer overflow in the packed PE file parsing implementation in BitDefender products before 20060829, including Antivirus

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	isa_server	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	ms_exchange_2000	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	ms_exchange_2003	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	ms_exchange_5.5	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	isa_server	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	ms_exchange_2000	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	ms_exchange_2003	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender</a>	ms_exchange_5.5	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Antivirus</a>	All	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Antivirus</a>	plus	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Antivirus</a>	All	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Antivirus</a>	plus	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Internet Security</a>	All	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Internet Security</a>	All	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Mail Protection</a>	enterprises	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Mail Protection</a>	enterprises	All	All	All
Application	<a href="#">Softwin</a>	<a href="#">Bitdefender Online Scanner</a>	All	All	All	All

Application	Softwin	Bitdefender Online Scanner	All	All	All	All
-------------	---------	----------------------------	-----	-----	-----	-----

## References

Reference	Source	Link
cevakrnl.xmd vulnerability	CONFIRM	<a href="#">www.b</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>
IBM X-Force Exchange	XF	<a href="#">exchar</a>
CXSecurity - IDS	SREASON	<a href="#">securit</a>
[Full-disclosure] BitDefender AV Packed PE File Parsing Engine Heap Overflow	FULLDISC	<a href="#">lists.gr</a>
BitDefender Heap Overflow in Parsing Packed PE Files Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">securit</a>
SecurityFocus	BUGTRAQ	<a href="#">www.s</a>
Multiple BitDefender Products Parsing Engine Integer Overflow Vulnerability	BID	<a href="#">www.s</a>
BitDefender AntiVirus Engine PE File Parsing Buffer Overflow - Advisories - Secunia	SECUNIA	<a href="#">secuni</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)