



# CVE-2014-9642

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

## Summary

<b>CVE</b>	CVE-2014-9642
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-02-06 15:59:00 UTC
<b>Updated</b>	2015-02-09 16:09:00 UTC
<b>Description</b>	bdagent.sys in BullGuard Antivirus, Internet Security, Premium Protection, and Online Backup before 15.0.288 allows local

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Bullguard</a>	<a href="#">Bdagent.sys</a>	All	All	All	All
Application	<a href="#">Bullguard</a>	<a href="#">Internet Security</a>	All	All	All	All
Application	<a href="#">Bullguard</a>	<a href="#">Online Backup</a>	All	All	All	All
Application	<a href="#">Bullguard</a>	<a href="#">Premium Protection</a>	All	All	All	All

## References

Reference	Source
Analysis Of An Interesting Windows Kernel Change Mitigating Vulnerabilities In Some Security Products   GreyHatHacker.NET	MISC
114478	OSVDB
BullGuard Multiple Products Arbitrary Write Privilege Escalation	EXPLOIT-DB
BullGuard 14.1.285.4 Privilege Escalation ≈ Packet Storm	MISC
Build 15.0.289	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)**