



# CVE-2009-3641

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2009-3641
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-10-28 14:30:00 UTC
<b>Updated</b>	2017-08-17 01:31:00 UTC
<b>Description</b>	Snort before 2.8.5.1, when the -v option is enabled, allows remote attackers to cause a denial of service (application crash)

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snort	Snort	1.6	All	All	All
Application	Snort	Snort	1.8.0	All	All	All
Application	Snort	Snort	1.8.1	All	All	All
Application	Snort	Snort	1.8.2	All	All	All
Application	Snort	Snort	1.8.3	All	All	All
Application	Snort	Snort	1.8.4	All	All	All
Application	Snort	Snort	1.8.5	All	All	All
Application	Snort	Snort	1.8.6	All	All	All
Application	Snort	Snort	1.8.7	All	All	All
Application	Snort	Snort	1.9.0	All	All	All
Application	Snort	Snort	1.9.1	All	All	All
Application	Snort	Snort	2.0	beta	All	All
Application	Snort	Snort	2.0	rc1	All	All
Application	Snort	Snort	2.6.1	All	All	All
Application	Snort	Snort	2.6.1.1	All	All	All
Application	Snort	Snort	2.6.1.2	All	All	All
Application	Snort	Snort	2.6.2	All	All	All

Application	Snort	Snort	2.7_beta1	All	All	All
Application	Snort	Snort	2.8.0	All	All	All
Application	Snort	Snort	2.8.2.2	All	All	All
Application	Snort	Snort	2.8.3	All	All	All
Application	Snort	Snort	2.8.3.1	All	All	All
Application	Snort	Snort	2.8.3.2	All	All	All
Application	Snort	Snort	2.8.3.4	All	All	All
Application	Snort	Snort	2.8.3.4.1	All	All	All
Application	Snort	Snort	1.6	All	All	All
Application	Snort	Snort	1.8.0	All	All	All
Application	Snort	Snort	1.8.1	All	All	All
Application	Snort	Snort	1.8.2	All	All	All
Application	Snort	Snort	1.8.3	All	All	All
Application	Snort	Snort	1.8.4	All	All	All
Application	Snort	Snort	1.8.5	All	All	All
Application	Snort	Snort	1.8.6	All	All	All
Application	Snort	Snort	1.8.7	All	All	All
Application	Snort	Snort	1.9.0	All	All	All
Application	Snort	Snort	1.9.1	All	All	All
Application	Snort	Snort	2.0	beta	All	All
Application	Snort	Snort	2.0	rc1	All	All
Application	Snort	Snort	2.6.1	All	All	All
Application	Snort	Snort	2.6.1.1	All	All	All
Application	Snort	Snort	2.6.1.2	All	All	All
Application	Snort	Snort	2.6.2	All	All	All
Application	Snort	Snort	2.7_beta1	All	All	All
Application	Snort	Snort	2.8.0	All	All	All
Application	Snort	Snort	2.8.2.2	All	All	All
Application	Snort	Snort	2.8.3	All	All	All
Application	Snort	Snort	2.8.3.1	All	All	All
Application	Snort	Snort	2.8.3.2	All	All	All
Application	Snort	Snort	2.8.3.4	All	All	All
Application	Snort	Snort	2.8.3.4.1	All	All	All
Application	Snort	Snort	All	All	All	All

## References

Reference	Source
VRT: Snort 2.8.5.1 Release	CONFIRM
About Secunia Research   Flexera	SECUNIA
Snort Bug in Monitoring IPv6 Data Lets Remote Users Deny Service - SecurityTracker	SECTRACK
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
oss-security - SANS: Security Thought LeadersRe: CVE Request -- Snort - 2.8.5.1	MLIST
Full Disclosure: Snort <= 2.8.5 IPV6 Remote DoS	FULLDISC
Just a moment...	CONFIRM
[oss-security] 20091025 CVE Request -- Snort - 2.8.5.1	MLIST
Snort Multiple Denial Of Service Vulnerabilities	BID
IBM X-Force Exchange	XF
530863 – (CVE-2009-3641) CVE-2009-3641 Snort: DoS (crash) while printing specially-crafted IPv6 packet using the -v option	CONFIRM
59159	OSVDB
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](#)