



# CVE-2023-0656

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

## Summary

<b>CVE</b>	CVE-2023-0656
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT@sonicwall.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-02 22:15:00 UTC
<b>Updated</b>	2023-03-10 21:04:00 UTC
<b>Description</b>	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Ser

## Risk And Classification

**Problem Types: CWE-787**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sonicwall	Nsa 2700	-	All	All	All
Hardware	Sonicwall	Nsa 3700	-	All	All	All
Hardware	Sonicwall	Nsa 4700	-	All	All	All
Hardware	Sonicwall	Nsa 5700	-	All	All	All
Hardware	Sonicwall	Nsa 6700	-	All	All	All
Hardware	Sonicwall	Nssp 10700	-	All	All	All
Hardware	Sonicwall	Nssp 11700	-	All	All	All
Hardware	Sonicwall	Nssp 13700	-	All	All	All
Hardware	Sonicwall	Nssp 15700	-	All	All	All
Hardware	Sonicwall	Nsv 10	-	All	All	All
Hardware	Sonicwall	Nsv 100	-	All	All	All
Hardware	Sonicwall	Nsv 1600	-	All	All	All
Hardware	Sonicwall	Nsv 200	-	All	All	All
Hardware	Sonicwall	Nsv 25	-	All	All	All
Hardware	Sonicwall	Nsv 270	-	All	All	All
Hardware	Sonicwall	Nsv 300	-	All	All	All
Hardware	Sonicwall	Nsv 400	-	All	All	All

Hardware	<a href="#">Sonicwall</a>	<a href="#">Nsv 470</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Nsv 50</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Nsv 800</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Nsv 870</a>	-	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sonicos</a>	All	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sonicos</a>	All	All	All	All
Operating System	<a href="#">Sonicwall</a>	<a href="#">Sonicos</a>	All	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz270</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz270w</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz370</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz370w</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz470</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz470w</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz570</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz570p</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz570w</a>	-	All	All	All
Hardware	<a href="#">Sonicwall</a>	<a href="#">Tz670</a>	-	All	All	All

## References

Reference	Source	Link	Tags
Security Advisory	CONFIRM	<a href="https://psirt.global.sonicwall.com">psirt.global.sonicwall.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[730766](#) SonicWall SONICOS Stack-Based Buffer Overflow Vulnerability (SNWLID-2023-0004)

© [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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)