



CVE-2015-4173

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

Summary

CVE	CVE-2015-4173
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-26 19:59:00 UTC
Updated	2020-08-05 15:04:00 UTC
Description	Unquoted Windows search path vulnerability in the autorun value in Dell SonicWall NetExtender before 7.5.227 and 8.0.x b

Risk And Classification

Problem Types: CWE-428

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonicwall	Netextender	All	All	All	All
Application	Sonicwall	Netextender	All	All	All	All

References

Reference	Source	Link
SSL-VPN NetExtender Product Notification	CONFIRM	support.softw...
SecurityFocus	BUGTRAQ	www.securityf...
Dell SonicWALL Extender Unquoted Search Path Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack	www.securityt...
Dell SonicWall NetExtender 7.5.215 Privilege Escalation ≈ Packet Storm	MISC	packetstorms...
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)