



CVE-2023-26237

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-26237
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-05 01:15:00 UTC
Updated	2023-10-11 14:00:00 UTC
Description	An issue was discovered in WatchGuard EPDR 8.0.21.0002. It is possible to bypass the defensive capabilities by adding a

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Watchguard	Edr	-	All	All	All
Operating System	Watchguard	Edr Firmware	All	All	All	All
Hardware	Watchguard	Epdr	-	All	All	All
Operating System	Watchguard	Epdr Firmware	All	All	All	All
Hardware	Watchguard	Epp	-	All	All	All
Operating System	Watchguard	Epp Firmware	All	All	All	All
Hardware	Watchguard	Panda Ad360	-	All	All	All
Operating System	Watchguard	Panda Ad360 Firmware	All	All	All	All

References

Reference	Source	Link
WatchGuard EPDR and AD360 Advanced Protection Bypass Vulnerability via Registry Key WatchGuard Technologies	CONFIRM	www.w
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

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](#).

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

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