



CVE-2012-6614

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

Summary

CVE	CVE-2012-6614
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-19 15:15:00 UTC
Updated	2023-04-26 19:27:00 UTC
Description	D-Link DSR-250N devices before 1.08B31 allow remote authenticated users to obtain "persistent root access" via the Busy

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dsr-250n	-	All	All	All
Hardware	D-link	Dsr-250n	-	All	All	All
Operating System	D-link	Dsr-250n Firmware	All	All	All	All
Operating System	D-link	Dsr-250n Firmware	All	All	All	All
Hardware	Dlink	Dsr-250n	-	All	All	All
Operating System	Dlink	Dsr-250n Firmware	All	All	All	All

References

Reference	Source	Link	Tags
D-Link DSR-250N Backdoor ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
D-Link DSR-250N Persistent Root Access - Hardware papers Exploit	MISC	www.exploit-db.com	Exploit
ftp2.dlink.com/PRODUCTS/DSR-250N/REVA/DSR-SERIES_RELEASE_NOTES_v3.14.pdf	CONFIRM	ftp2.dlink.com	Release
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)