



CVE-2010-2892

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2010-2892
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-15 21:00:00 UTC
Updated	2018-10-10 20:00:00 UTC
Description	gsb/drivers.php in LANDesk Management Gateway 4.0 through 4.0-1.48 and 4.2 through 4.2-1.8 allows remote authenticat

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Landesk	Management Gateway	4.0	All	All	All
Hardware	Landesk	Management Gateway	4.0-1.48	All	All	All
Hardware	Landesk	Management Gateway	4.2	All	All	All
Hardware	Landesk	Management Gateway	4.2-1.8	All	All	All
Hardware	Landesk	Management Gateway	4.0	All	All	All
Hardware	Landesk	Management Gateway	4.0-1.48	All	All	All
Hardware	Landesk	Management Gateway	4.2	All	All	All
Hardware	Landesk	Management Gateway	4.2-1.8	All	All	All

References

Reference

[Landesk OS command injection](#)

[LANDesk Management Gateway Cross-Site Request Forgery Vulnerability - Advisories - Community](#)

[Core Security Technologies](#)

[LANDesk Management Gateway 'DRIVES' Parameter Remote Command Execution Vulnerability](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[LANDesk User Community: 11-10-2010 Vulnerability in the LANDesk Management Gateway](#)

SecurityFocus

SecurityTracker.com Archives - LANDesk Management Gateway Input Validation Error Lets Remote Authenticated Administrators Injection Op

CVE Program record

NVD vulnerability detail



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](#)