



CVE-2008-2468

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

Summary

CVE	CVE-2008-2468
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-18 15:04:00 UTC
Updated	2018-10-11 20:41:00 UTC
Description	Multiple buffer overflows in the QIP Server Service (aka qipsrvr.exe) in LANdesk Management Suite, Security Suite, and S

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Landesk	Landesk Management Suite	8.7	All	All	All
Application	Landesk	Landesk Management Suite	8.7	All	All	All
Application	Landesk	Landesk Management Suite	All	All	All	All
Application	Landesk	Landesk Security Suite	8.7	All	All	All
Application	Landesk	Landesk Security Suite	8.7	All	All	All
Application	Landesk	Landesk Security Suite	All	All	All	All
Application	Landesk	Landesk Server Manager	8.7	All	All	All
Application	Landesk	Landesk Server Manager	8.7	All	All	All
Application	Landesk	Landesk Server Manager	All	All	All	All

References

Reference	Source
LANdesk Management Suite Heap Overflow in the QIP Server Service Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECT
TippingPoint DV Labs	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
SecurityFocus	BUGT
IBM X-Force Exchange	XF

US-CERT Vulnerability Note VU#538011	CERT
LANDesk Intel QIP Service 'qipsrvr.exe' Buffer Overflow Vulnerability	BID
LANDesk Technical Community: Vulnerability in Intel QIP Service	CONF
LANDesk Multiple Products Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECU
SecurityReason - Landesk QIP Server Service Heal Packet Buffer Overflow	SREA
CVE Program record	CVE.C
NVD vulnerability detail	NVD



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](#)