CVE-2008-0525

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-0525
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-31 20:00:00 UTC
Updated	2018-10-15 22:00:00 UTC
Description	PatchLink Update client for Unix, as used by Novell ZENworks Patch Management Update Agent for Linux/Unix/Mac (LUM)

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lumension Security	Patchlink Update	6.2	All	linux	All
Application	Lumension Security	Patchlink Update	6.2	All	mac	All
Application	Lumension Security	Patchlink Update	6.2	All	unix	All
Application	Lumension Security	Patchlink Update	6.3	All	linux	All
Application	Lumension Security	Patchlink Update	6.3	All	mac	All
Application	Lumension Security	Patchlink Update	6.3	All	unix	All
Application	Lumension Security	Patchlink Update	6.4	All	linux	All
Application	Lumension Security	Patchlink Update	6.4	All	mac	All
Application	Lumension Security	Patchlink Update	6.4	All	unix	All
Application	Lumension Security	Patchlink Update	6.2	All	linux	All
Application	Lumension Security	Patchlink Update	6.2	All	mac	All
Application	Lumension Security	Patchlink Update	6.2	All	unix	All
Application	Lumension Security	Patchlink Update	6.3	All	linux	All
Application	Lumension Security	Patchlink Update	6.3	All	mac	All
Application	Lumension Security	Patchlink Update	6.3	All	unix	All
Application	Lumension Security	Patchlink Update	6.4	All	linux	All
Application	Lumension Security	Patchlink Update	6.4	All	mac	All

Application	Lumension Security	Patchlink Update	6.4	All	unix	All
Application	Novell	Zenworks Patch Management Update Agent	6.2	All	linux	All
Application	Novell	Zenworks Patch Management Update Agent	6.2	All	mac	All
Application	Novell	Zenworks Patch Management Update Agent	6.2	All	unix	All
Application	Novell	Zenworks Patch Management Update Agent	6.3	All	linux	All
Application	Novell	Zenworks Patch Management Update Agent	6.3	All	mac	All
Application	Novell	Zenworks Patch Management Update Agent	6.3	All	unix	All
Application	Novell	Zenworks Patch Management Update Agent	6.4	All	linux	All
Application	Novell	Zenworks Patch Management Update Agent	6.4	All	mac	All
Application	Novell	Zenworks Patch Management Update Agent	6.4	All	unix	All
Application	Novell	Zenworks Patch Management Update Agent	6.2	All	linux	All
Application	Novell	Zenworks Patch Management Update Agent	6.2	All	mac	All
Application	Novell	Zenworks Patch Management Update Agent	6.2	All	unix	All
Application	Novell	Zenworks Patch Management Update Agent	6.3	All	linux	All
Application	Novell	Zenworks Patch Management Update Agent	6.3	All	mac	All
Application	Novell	Zenworks Patch Management Update Agent	6.3	All	unix	All
Application	Novell	Zenworks Patch Management Update Agent	6.4	All	linux	All
Application	Novell	Zenworks Patch Management Update Agent	6.4	All	mac	All
Application	Novell	Zenworks Patch Management Update Agent	6.4	All	unix	All
Operating System	Unix	Unix	All	All	All	All
Operating System	Unix	Unix	All	All	All	All

References

Reference	Source	Li
CXSecurity - IDS	SREASON	se
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	w
PatchLink Update Temporary File Symlink Flaw in logtrimmer Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	w
support.lumension.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php	CONFIRM	su
secure-support.novell.com/KanisaPlatform/Publishing/18/3908994_f.SAL_Public.html	CONFIRM	se
IBM X-Force Exchange	XF	ex
PatchLink Update Client for Unix Insecure Temporary Files - Advisories - Secunia	SECUNIA	se
IBM X-Force Exchange	XF	ex
Novell ZENworks Patch Management Insecure Temporary Files - Advisories - Secunia	SECUNIA	se
SecurityFocus	BUGTRAQ	w
support.lumension.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php	CONFIRM	su

PatchLink Update Multiple Insecure Temporary File Creation Vulnerabilities	BID	w
support.lumension.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php	CONFIRM	su
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

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 registred 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**