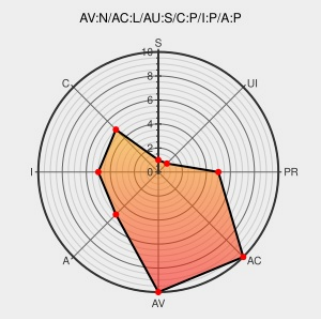
CVE-2005-4147

Published on: 12/10/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4147

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Listmanager from Lyris Technologies Inc contain the following vulnerability:

The TCLHTTPd service in Lyris ListManager before 8.9b allows remote attackers to obtain source code for arbitrary .tml (TCL) files via (1) a request with a trailing null byte (%00), which might also require (2) an authentication bypass step that involves a username with a trailing "@" characters.

CVE-2005-4147 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Neohapsis Archives - Full Disclosure List - #0349 - [Full-disclosure] PGP Wipe Free Space, Lyris ListManager Flaws, Windows Timestamps, Sam Juicer	web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20051208 PGP Wipe Free Space, Lyris ListManager Flaws, Windows Timestamps, Sam Juicer
The Metasploit Project	Exploit, Patch, web.archive.org, text/html, Inactive Link, Not Archived	MISC metasploit.com/research/vulns/lyris_listmanager/
Lyris Listmanager TCLHTTPd Service Multiple Information Disclosure Vulnerabilities	Patch, cve.report (archive), text/html	BID 15788
No Description Provided	Exploit	OSVDB 21551

	Patch www.osvdb.org Inactive Link Not Archived	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-2820
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051209 PGP Wipe Free Space, Lyris ListManager Flaws, Windows Timestamps, Sam Juicer
No Description Provided	Exploit Patch www.osvdb.org Inactive Link Not Archived	OSVDB 21573
Secunia - Advisories - Lyris ListManager Multiple Vulnerabilities	Exploit Patch Vendor Advisory web.archive.org text/html	SECUNIA 17943

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lyris Technologies Inc	Listmanager	5.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	6.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	7.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	8.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	8.8a	All	All	All
Application	Lyris Technologies Inc	Listmanager	5.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	6.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	7.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	8.0	All	All	All
Application	Lyris Technologies Inc	Listmanager	8.8a	All	All	All

cpe:2.3:a:lyris_technologies_inc:listmanager:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:lyris_technologies_inc:listmanager:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:lyris_technologies_inc:listmanager:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:lyris_technologies_inc:listmanager:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:lyris_technologies_inc:listmanager:8.8a:*:*:*:*:*:*:*

cpe:2.3:a:lyris_technologies_inc:listmanager:5.0:*:*:*:*:*:*:*

cpe:2.3:a:lyris_technologies_inc:listmanager:6.0:*:*:*:*:*:*:*

cpe:2.3:a:lyris_technologies_inc:listmanager:7.0:*:*:*:*:*:*:*

cpe:2.3:a:lyris_technologies_inc:listmanager:8.0:*:*:*:*:*:*:*

cpe:2.3:a:lyris_technologies_inc:listmanager:8.8a:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→