



# CVE-2005-3120

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2005-3120
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-10-17 20:06:00 UTC
<b>Updated</b>	2024-02-02 14:00:00 UTC
<b>Description</b>	Stack-based buffer overflow in the HTrjjs function in Lynx 2.8.6 and earlier allows remote NNTP servers to execute arbitrary

## Risk And Classification

**Problem Types: CWE-131**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	All	All
Application	<a href="#">Invisible-island</a>	<a href="#">Lynx</a>	All	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.3	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.4	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.6	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.6_dev13	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.3	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.4	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.6	All	All	All
Application	<a href="#">University Of Kansas</a>	<a href="#">Lynx</a>	2.8.6_dev13	All	All	All

## References

Reference	
Secunia - Advisories - Debian update for lynx	S
USN-206-1: Lynx vulnerability   Ubuntu security notices	U
The Slackware Linux Project: Slackware Security Advisories	S

Debian update for lynx-cur - Advisories - Secunia	S
Secunia - Advisories - Gentoo update for lynx	S
Secunia - Advisories - Lynx "HTrjis()" NNTP Buffer Overflow Vulnerability	S
Secunia - Advisories - UnixWare update for lynx	S
SecurityTracker.com Archives - Lynx Buffer Overflow in HTrjis() in Processing NNTP Headers Lets Remote Users Execute Arbitrary Code	S
Secunia - Advisories - Avaya S87XX/S8500/S8300 Lynx "HTrjis()" NNTP Buffer Overflow	S
Gentoo Linux Documentation -- Lynx: Buffer overflow in NNTP processing	C
SecurityFocus	E
Secunia - Advisories - Debian update for lynx-ssl	S
Secunia - Advisories - Slackware update for lynx	S
Advisories - Mandriva	M
TLSA-2005-0059 - multi	T
SCOSA-2006.7	S
Secunia - Advisories - SCO OpenServer update for lynx	S
Security Announcement	S
Secunia - Advisories - Fedora update for lynx	S
170253 – (CVE-2005-3120) CAN-2005-3120 lynx buffer overflow	M
Secunia - Advisories - Red Hat update for lynx	S
SecurityFocus	F
Lynx NNTP Article Header Buffer Overflow Vulnerability	E
OpenPKG Project: Security: Security Advisories	C
Debian -- Security Information -- DSA-876-1 lynx-ssl	D
SCOSA-2005.47	S
1. Overview:	C
Debian -- Security Information -- DSA-1085-1 lynx-cur	D
Secunia - Advisories - Mandriva update for lynx	S
Repository / Oval Repository	C
Secunia - Advisories - SUSE Updates for Multiple Packages	S
rhn.redhat.com   Red Hat Support	F
Secunia - Advisories - Ubuntu update for lynx	S
[Full-disclosure] Lynx Remote Buffer Overflow	F
Debian -- Security Information -- DSA-874-1 lynx	D
CVE Program record	C
NVD vulnerability detail	N

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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](#)