CVE-2005-3120

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2005-3120
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-17 20:06:00 UTC
Updated	2024-02-02 14:00:00 UTC
Description	Stack-based buffer overflow in the HTrjis 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	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Application	Invisible-island	Lynx	All	All	All	All
Application	University Of Kansas	Lynx	2.8.3	All	All	All
Application	University Of Kansas	Lynx	2.8.4	All	All	All
Application	University Of Kansas	Lynx	2.8.6	All	All	All
Application	University Of Kansas	Lynx	2.8.6_dev13	All	All	All
Application	University Of Kansas	Lynx	2.8.3	All	All	All
Application	University Of Kansas	Lynx	2.8.4	All	All	All
Application	University Of Kansas	Lynx	2.8.6	All	All	All
Application	University Of Kansas	Lynx	2.8.6_dev13	All	All	All

References

Reference	S
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	G
SecurityFocus	B
Secunia - Advisories - Debian update for lynx-ssl	S
Secunia - Advisories - Slackware update for lynx	S
Advisories - Mandriva	M
TSLSA-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	B
OpenPKG Project: Security: Security Advisories	O
Debian -- Security Information -- DSA-876-1 lynx-ssl	D
SCOSA-2005.47	S
1. Overview:	O
Debian -- Security Information -- DSA-1085-1 lynx-cur	D
Secunia - Advisories - Mandriva update for lynx	S
Repository / Oval Repository	O
Secunia - Advisories - SUSE Updates for Multiple Packages	S
rhn.redhat.com | Red Hat Support	R
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

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.