



CVE-2004-1617

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

Summary

CVE	CVE-2004-1617
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-10-18 04:00:00 UTC
Updated	2018-10-19 15:30:00 UTC
Description	Lynx, lynx-ssl, and lynx-cur before 2.8.6dev.8 allow remote attackers to cause a denial of service (infinite loop) via a web page

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	University Of Kansas	Lynx	2.7	All	All	All
Application	University Of Kansas	Lynx	2.8	All	All	All
Application	University Of Kansas	Lynx	2.8.1	All	All	All
Application	University Of Kansas	Lynx	2.8.2_rel1	All	All	All
Application	University Of Kansas	Lynx	2.8.3	All	All	All
Application	University Of Kansas	Lynx	2.8.3_dev22	All	All	All
Application	University Of Kansas	Lynx	2.8.3_pre5	All	All	All
Application	University Of Kansas	Lynx	2.8.3_rel1	All	All	All
Application	University Of Kansas	Lynx	2.8.4	All	All	All
Application	University Of Kansas	Lynx	2.8.4_rel1	All	All	All
Application	University Of Kansas	Lynx	2.8.5	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev2	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev3	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev4	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev5	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev8	All	All	All
Application	University Of Kansas	Lynx	2.7	All	All	All

Application	University Of Kansas	Lynx	2.8	All	All	All
Application	University Of Kansas	Lynx	2.8.1	All	All	All
Application	University Of Kansas	Lynx	2.8.2_rel1	All	All	All
Application	University Of Kansas	Lynx	2.8.3	All	All	All
Application	University Of Kansas	Lynx	2.8.3_dev22	All	All	All
Application	University Of Kansas	Lynx	2.8.3_pre5	All	All	All
Application	University Of Kansas	Lynx	2.8.3_rel1	All	All	All
Application	University Of Kansas	Lynx	2.8.4	All	All	All
Application	University Of Kansas	Lynx	2.8.4_rel1	All	All	All
Application	University Of Kansas	Lynx	2.8.5	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev2	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev3	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev4	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev5	All	All	All
Application	University Of Kansas	Lynx	2.8.5_dev8	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-1076-1 lynx	DEBIAN	www.debian.org
Lynx Malformed HTML Infinite Loop Denial Of Service Vulnerability	BID	www.securityfocus.com
Debian update for lynx-cur - Advisories - Secunia	SECUNIA	secunia.com
SecurityTracker.com Archives - Lynx HTML Parsing Errors Let Remote Users Deny Service	SECTRACK	securitytracker.com
[Full-Disclosure] Web browsers - a mini-farce	FULLDISC	lists.grok.org.uk
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
'Web browsers - a mini-farce' - MARC	BUGTRAQ	marc.info
wrong number (404)	MISC	lcamtuf.coredump.cx
Debian -- Security Information -- DSA-1077-1 lynx-ssl	DEBIAN	www.debian.org
Debian -- Security Information -- DSA-1085-1 lynx-cur	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)