



CVE-2008-2021

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-2021
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-30 12:05:00 UTC
Updated	2017-08-08 01:30:00 UTC
Description	Heap-based buffer overflow in Lhaplus before 1.57 allows remote attackers to execute arbitrary code via a long comment fi

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lhaplus	Lhaplus	All	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xfo
www.fourteenforty.jp/research/advisory.cgi	MISC	www.fourteen
www7a.biglobe.ne.jp/~schezo	CONFIRM	www7a.biglot
Lhaplus ZOO Archive Processing Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.c
JVN#74468481: Lhaplus におけるバッファオーバーフローの脆弱性	JVN	jvn.jp
Lhaplus ZOO Archive Processing Remote Buffer Overflow Vulnerability	BID	www.security
JVN:JVN#74468481	MITRE	jvn.jp
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)