



CVE-2008-3895

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2008-3895
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-03 14:12:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	LILO 22.6.1 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lilo	Lilo	0	All	All	All

Application	Lilo	Lilo	1	All	All	All
Application	Lilo	Lilo	10	All	All	All
Application	Lilo	Lilo	11	All	All	All
Application	Lilo	Lilo	12	All	All	All
Application	Lilo	Lilo	13	All	All	All
Application	Lilo	Lilo	14	All	All	All
Application	Lilo	Lilo	15	All	All	All
Application	Lilo	Lilo	16	All	All	All
Application	Lilo	Lilo	17	All	All	All
Application	Lilo	Lilo	18	All	All	All
Application	Lilo	Lilo	19	All	All	All
Application	Lilo	Lilo	2	All	All	All
Application	Lilo	Lilo	20	All	All	All
Application	Lilo	Lilo	21	All	All	All
Application	Lilo	Lilo	21-3	All	All	All
Application	Lilo	Lilo	21.4.2	All	All	All
Application	Lilo	Lilo	21.4.3	All	All	All
Application	Lilo	Lilo	21.4.4	All	All	All
Application	Lilo	Lilo	21.5	All	All	All
Application	Lilo	Lilo	21.5.1	All	All	All
Application	Lilo	Lilo	21.6	All	All	All
Application	Lilo	Lilo	21.6.1	All	All	All
Application	Lilo	Lilo	21.7	All	All	All
Application	Lilo	Lilo	21.7.1	All	All	All
Application	Lilo	Lilo	21.7.2	All	All	All
Application	Lilo	Lilo	21.7.3	All	All	All
Application	Lilo	Lilo	21.7.4	All	All	All
Application	Lilo	Lilo	21.7.5	All	All	All
Application	Lilo	Lilo	22.0	All	All	All
Application	Lilo	Lilo	22.0.1	All	All	All
Application	Lilo	Lilo	22.0.2	All	All	All
Application	Lilo	Lilo	22.1	All	All	All
Application	Lilo	Lilo	22.2	All	All	All
Application	Lilo	Lilo	22.3	All	All	All
Application	Lilo	Lilo	22.3.1	All	All	All
Application	Lilo	Lilo	22.3.2	All	All	All

Application	Lilo	Lilo	22.3.3	All	All	All
Application	Lilo	Lilo	22.3.4	All	All	All
Application	Lilo	Lilo	22.4	All	All	All
Application	Lilo	Lilo	22.4.1	All	All	All
Application	Lilo	Lilo	22.5	All	All	All
Application	Lilo	Lilo	22.5.1	All	All	All
Application	Lilo	Lilo	22.5.2	All	All	All
Application	Lilo	Lilo	22.5.3	All	All	All
Application	Lilo	Lilo	22.5.3.1	All	All	All
Application	Lilo	Lilo	22.5.4	All	All	All
Application	Lilo	Lilo	22.5.5	All	All	All
Application	Lilo	Lilo	22.5.6	All	All	All
Application	Lilo	Lilo	22.5.7	All	All	All
Application	Lilo	Lilo	22.5.7.2	All	All	All
Application	Lilo	Lilo	22.5.8	All	All	All
Application	Lilo	Lilo	22.5.9	All	All	All
Application	Lilo	Lilo	22.6	All	All	All
Application	Lilo	Lilo	3	All	All	All
Application	Lilo	Lilo	4	All	All	All
Application	Lilo	Lilo	5	All	All	All
Application	Lilo	Lilo	6	All	All	All
Application	Lilo	Lilo	7	All	All	All
Application	Lilo	Lilo	8	All	All	All
Application	Lilo	Lilo	9	All	All	All
Application	Lilo	Lilo	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source		Link	
iViZ - On Demand Automated Penetration Testing			af854a3a-2127-422b-91ae-364da2661108		www.ivizsecu	
SecurityFocus			af854a3a-2127-422b-91ae-364da2661108		www.security	
SecurityReason - LILO Security Model bypass exploiting wrong BIOS API usage			af854a3a-2127-422b-91ae-364da2661108		securityreaso	
www.ivizsecurity.com/research/preboot/preboot_whitepaper.pdf			af854a3a-2127-422b-91ae-364da2661108		www.ivizsecu	

CVE Program record

CVE.ORG

www.cve.org

NVD vulnerability detail

NVD

nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-01-29	Joshua Bressers	Red Hat does not consider this to be a security issue. Since these operations can only be e

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