CVE-2008-3896

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

Summary

CVE	CVE-2008-3896
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	Grub Legacy 0.97 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this

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	Gnu	Grub Legacy	0.92	All	All	All

Application	Gnu	Grub Legacy	0.93	All	All	All
Application	Gnu	Grub Legacy	0.94	All	All	All
Application	Gnu	Grub Legacy	0.94-i386-pc	All	All	All
Application	Gnu	Grub Legacy	0.95	All	All	All
Application	Gnu	Grub Legacy	0.95-i386-pc	All	All	All
Application	Gnu	Grub Legacy	0.96	All	All	All
Application	Gnu	Grub Legacy	0.96-i386-pc	All	All	All
Application	Gnu	Grub Legacy	0.97-i386-pc	All	All	All
Application	Gnu	Grub Legacy	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
Grub Legacy Security Model bypass exploiting wrong BIOS API usage - CXSecurity.com	af854a3a-2127-422b-91ae-364da2661108	secu
iViZ - On Demand Automated Penetration Testing	af854a3a-2127-422b-91ae-364da2661108	www
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www
CXSecurity.com - IT Security News	af854a3a-2127-422b-91ae-364da2661108	secu
www.ivizsecurity.com/research/preboot/preboot_whitepaper.pdf	af854a3a-2127-422b-91ae-364da2661108	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

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 ex

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report