



CVE-2016-1885

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

Summary

CVE	CVE-2016-1885
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-12 02:00:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Integer signedness error in the amd64_set_ldt function in sys/amd64/amd64/sys_machdep.c in FreeBSD 9.3 before p39, 10

Risk And Classification

Primary CVSS: v3.0 6.2 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	6.2	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.9		AV:L/AC:L/Au:N/C:N/I:N/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	10.1	All	All	All
Operating System	Freebsd	Freebsd	10.2	All	All	All
Operating System	Freebsd	Freebsd	9.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Full Disclosure: Re: [CORE-2016-0005] - FreeBSD Kernel amd64_set_ldt Heap Overflow	af8
Full Disclosure: [CORE-2016-0005] - FreeBSD Kernel amd64_set_ldt Heap Overflow	af8
SecurityFocus	af8
FreeBSD Kernel amd64_set_ldt Heap Overflow Core Security	af8
FreeBSD Kernel amd64_set_ldt Heap Overflow ≈ Packet Storm	af8
SecurityFocus	af8
FreeBSD sysarch(2) Input Validation Flaw Lets Local Users Cause Denial of Service Conditions on the Target System - SecurityTracker	af8
FreeBSD 10.2 (x64) - 'amd64_set_ldt' Heap Overflow - FreeBSD_x86-64 dos Exploit	af8

security.FreeBSD.org/advisories/FreeBSD-SA-16:15.sysarch.asc	af8
CVE Program record	CV
NVD vulnerability detail	NV
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](#)