



CVE-2009-0115

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2009-0115
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-30 16:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Device Mapper multipathing driver (aka multipath-tools or device-mapper-multipath) 0.4.8, as used in SUSE openSUSE

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-732 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Intuity Audix Lx	2.0	-	All	All
Application	Avaya	Intuity Audix Lx	2.0	sp1	All	All
Application	Avaya	Intuity Audix Lx	2.0	sp2	All	All
Application	Avaya	Message Networking	3.1	All	All	All
Application	Avaya	Messaging Storage Server	3.0	All	All	All
Application	Avaya	Messaging Storage Server	4.0	All	All	All
Application	Avaya	Messaging Storage Server	5.0	All	All	All
Application	Christophe.varoqui	Multipath-tools	0.4.8	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Fedoraproject	Fedora	10	All	All	All
Operating System	Fedoraproject	Fedora	9	All	All	All
Application	Juniper	Ctpview	All	All	All	All
Application	Juniper	Ctpview	7.1	-	All	All
Operating System	Novell	Open Enterprise Server	-	All	All	All
Operating System	Opensuse	Opensuse	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	9	All	All	All

Operating System	Suse	Linux Enterprise Server	10	-	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Fedora update for device-mapper-multipath - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-42
Debian -- Security Information -- DSA-1767-1 multipath-tools	af854a3a-2127-42
SUSE Update for Multiple Packages - Advisories - Community	af854a3a-2127-42
VMware vMA Update for Multiple Packages - Advisories - Community	af854a3a-2127-42
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:007	af854a3a-2127-42
Resource is no longer available!	af854a3a-2127-42
Repository / Oval Repository	af854a3a-2127-42
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-42
[SECURITY] Fedora 9 Update: device-mapper-multipath-0.4.7-17.fc9	af854a3a-2127-42
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-42
[Security-announce] VMSA-2010-0004 ESX Service Console and vMA third party updates	af854a3a-2127-42
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:008	af854a3a-2127-42
CVE-2009-0115	af854a3a-2127-42
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	af854a3a-2127-42
Debian update for multipath-tools - Secunia.com	af854a3a-2127-42
ASA-2009-128 (RHSA-2009-0411)	af854a3a-2127-42
Avaya Products device-mapper-multipath Insecure Socket - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-42
2015-07 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	af854a3a-2127-42
[SECURITY] Fedora 10 Update: device-mapper-multipath-0.4.8-9.fc10	af854a3a-2127-42
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)