



CVE-2013-2147

Published on: 06/07/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

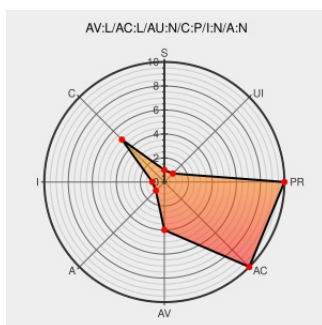
CVE-2013-2147

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

The HP Smart Array controller disk-array driver and Compaq SMART2 controller disk-array driver in the Linux kernel through 3.9.4 do not initialize certain data structures, which allows local users to obtain sensitive information from kernel memory via (1) a crafted IDAGETPCIINFO command for a /dev/ida device, related to the ida_locked_ioctl function in drivers/block/cpqarray.c or (2) a crafted CCISS_PASSTHRU32 command for a /dev/cciss device, related to the cciss_ioctl32_passthru function in drivers/block/cciss.c.

CVE-2013-2147 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

[security-announce] SUSE-SU-2015:0812-1:
important: Security update for

[lists.opensuse.org](#)
[text/html](#)

[SUSE SUSE-SU-2015:0812](#)

USN-1997-1: Linux kernel (OMAP4) vulnerability |
Ubuntu

[www.ubuntu.com](#)
[text/html](#)

[UBUNTU USN-1997-1](#)

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2013:1166](#)

USN-1996-1: Linux kernel vulnerability | Ubuntu

[www.ubuntu.com](#)

[UBUNTU USN-1996-1](#)

CVE-1999-1: Linux kernel vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU CVE-1999-1
USN-2020-1: Linux kernel (Raring HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2020-1
Bug 971242 – CVE-2013-2147 Kernel: cpqarray/cciss: information leak via ioctl	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=971242
USN-2015-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2015-1
LKML: Dan Carpenter: [patch] cpqarray: info leak in ida_locked_ioctl()	lkml.org text/xml	 MLIST [linux-kernel] 20130603 [patch] cpqarray: info leak in ida_locked_ioctl()
LKML: Dan Carpenter: [patch] cciss: info leak in cciss_ioctl32_passthru()	lkml.org text/xml	 MLIST [linux-kernel] 20130603 [patch] cciss: info leak in cciss_ioctl32_passthru()
USN-2050-1: Linux kernel (OMAP4) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2050-1
USN-2016-1: Linux kernel (EC2) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2016-1
USN-2023-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2023-1
oss-security - Re: CVE request: kernel: cpqarray/c: info leak in ida_locked_ioctl()	www.openwall.com text/html	 MLIST [oss-security] 20130605 Re: CVE request: kernel: cpqarray/c: info leak in ida_locked_ioctl()
USN-1999-1: Linux kernel (OMAP4) vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1999-1
USN-2017-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2017-1
USN-1994-1: Linux kernel (Quantal HWE) vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1994-1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.9	rc1	All	All
Operating System	Linux	Linux Kernel	3.9	rc2	All	All
Operating System	Linux	Linux Kernel	3.9	rc3	All	All
Operating System	Linux	Linux Kernel	3.9	rc4	All	All
Operating System	Linux	Linux Kernel	3.9	rc5	All	All

Operating System	Linux	Linux Kernel	3.9	rc6	All	All
Operating System	Linux	Linux Kernel	3.9	rc7	All	All
Operating System	Linux	Linux Kernel	3.9.0	All	All	All
Operating System	Linux	Linux Kernel	3.9.1	All	All	All
Operating System	Linux	Linux Kernel	3.9.2	All	All	All
Operating System	Linux	Linux Kernel	3.9.3	All	All	All
Operating System	Linux	Linux Kernel	3.9	rc1	All	All
Operating System	Linux	Linux Kernel	3.9	rc2	All	All
Operating System	Linux	Linux Kernel	3.9	rc3	All	All
Operating System	Linux	Linux Kernel	3.9	rc4	All	All
Operating System	Linux	Linux Kernel	3.9	rc5	All	All
Operating System	Linux	Linux Kernel	3.9	rc6	All	All
Operating System	Linux	Linux Kernel	3.9	rc7	All	All
Operating System	Linux	Linux Kernel	3.9.0	All	All	All
Operating System	Linux	Linux Kernel	3.9.1	All	All	All
Operating System	Linux	Linux Kernel	3.9.2	All	All	All
Operating System	Linux	Linux Kernel	3.9.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
cpe:2.3:o:linux:linux_kernel:3.9:rc1:::~::~:						
cpe:2.3:o:linux:linux_kernel:3.9:rc2::~::~:						
cpe:2.3:o:linux:linux_kernel:3.9:rc3::~::~:						
cpe:2.3:o:linux:linux_kernel:3.9:rc4::~::~:						

cpe:2.3:o:linux:linux_kernel:3.9:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.0:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc6:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9:rc7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.0:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:3.9.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp4:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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