



CVE-2016-3699

Published on: 10/07/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:50:00 AM UTC

CVE-2016-3699

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The Linux kernel, as used in Red Hat Enterprise Linux 7.2 and Red Hat Enterprise MRG 2 and when booted with UEFI Secure Boot enabled, allows local users to bypass intended Secure Boot restrictions and execute untrusted code by appending ACPI tables to the initrd.

CVE-2016-3699 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.4 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:2574
acpi: Disable ACPI table override if securelevel is set	Exploit github.com	MISC github.com/mjg59/linux/commit/a4a5ed2835e8ea042868b7401dced3f517cafa76

· mjpg59/linux@a4a5ed2 · GitHub	text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2574
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2016:2584
Red Hat Enterprise Linux CVE-2016-3699 Local Security Bypass Vulnerability	Broken Link cve.report (archive) text/html	 BID 93114
Bug 1329653 – CVE-2016-3699 kernel: ACPI table override allowed when securelevel is enabled	Issue Tracking Patch Third Party Advisory VDB Entry bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1329653
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2584
CVE-2016-3699 - Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2016-3699
oss-security - kernel: ACPI table override is allowed when securelevel is enabled	Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20160922 kernel: ACPI table override is allowed when securelevel is enabled

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	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Enterprise Mrg	2.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Linux	7.2	All	All	All
Operating System	Redhat	Linux	7.2	All	All	All

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:
cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_mrg:2.0:*:*:*:*:*:
cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2:*:*:*:*:*:
cpe:2.3:o:redhat:linux:7.2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)