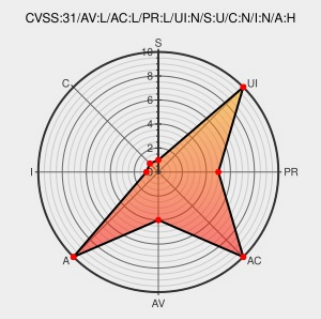
CVE-2007-3732

Published on: 11/07/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:40 AM UTC

CVE-2007-3732

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

In Linux 2.6 before 2.6.23, the TRACE_IRQS_ON function in iret_exc calls a C function without ensuring that the segments are set properly. The kernel's %fs needs to be restored before the call in TRACE_IRQS_ON and before enabling interrupts, so that "current" references work. Without this, "current" used in the window between iret_exc and the middle of error_code where %fs is reset, would crash.

CVE-2007-3732 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **linux-2.6** - **linux-2.6** version **= 2.6 before 2.6.23**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link

Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2007-3732
CVE-2007-3732	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2007-3732
248353 – (CVE-2007-3732) CVE-2007-3732 kernel: Reset %fs early in iret_exc	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2007-3732

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	All
Operating System	Linux	Linux Kernel	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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