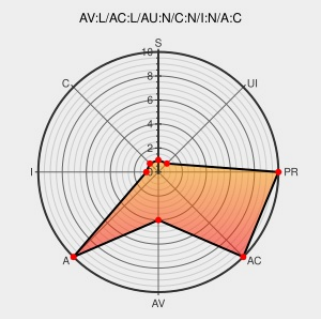
# CVE-2010-1436

Published on: 05/21/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:17:00 AM UTC

## CVE-2010-1436

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




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

gfs2 in the Linux kernel 2.6.18, and possibly other versions, does not properly handle when the gfs2_quota struct occupies two separate pages, which allows local users to cause a denial of service (kernel panic) via certain manipulations that cause an out-of-bounds write, as demonstrated by writing from an ext3 file system to a gfs2 file system.

CVE-2010-1436 has been assigned by secalert@redhat.com to track the vulnerability

### CVSS2 Score: 4.9 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| SecurityFocus | www.securityfocus.com text/html | BUGTRAQ 20110211 VMSA-2011-0003 Third party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX |
| Repository / Oval Repository | oval.cisecurity.org text/html | OVAL oval:org.mitre.oval:def:10652 |
| VMSA-2011-0003 | www.vmware.com text/html | CONFIRM www.vmware.com/security/advisories/VMSA-2011-0003.html |
| Red Hat Customer Portal | access.redhat.com text/html | MISC access.redhat.com/errata/RHSA-2010:0504 |
| oss-security - CVE request - gfs2 kernel issue | www.openwall.com text/html | MLIST [oss-security] 20100427 CVE request - gfs2 kernel issue |

| | | |
|---|---|---|
| oss-security - Re: CVE request - gfs2 kernel issue | www.openwall.com<br>text/html | MLIST [oss-security] 20100427 Re: CVE request - gfs2 kernel issue |
| VMware ESX Server Multiple Kernel Vulnerabilities - Advisories - Community | web.archive.org<br>text/html | SECUNIA 43315 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF kernel-gfs2quota-dos(58839) |
| access.redhat.com \| CVE-2010-1436 | access.redhat.com<br>text/html | MISC access.redhat.com/security/cve/CVE-2010-1436 |
| Bug 586006 – CVE-2010-1436 kernel: gfs2 buffer overflow | Exploit<br>bugzilla.redhat.com<br>text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=586006 |

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 | 2.6.18 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.18 | All | All | All |

cpe:2.3:o:linux:linux_kernel:2.6.18:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.18:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→