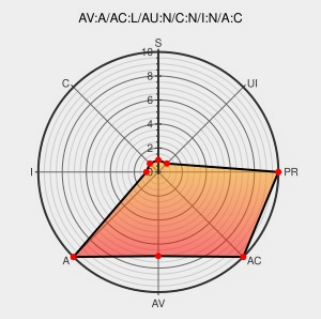
# CVE-2011-1780

Published on: 01/07/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:19 AM UTC

## CVE-2011-1780

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




Certain versions of Xen from Xen contain the following vulnerability:

The instruction emulation in Xen 3.0.3 allows local SMP guest users to cause a denial of service (host crash) by replacing the instruction that causes the VM to exit in one thread with a different instruction in a different thread.

CVE-2011-1780 has been assigned by secalert@redhat.com to track the vulnerability

### CVSS2 Score: 6.1 - MEDIUM

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| Bug 702657 – CVE-2011-1780 kernel: xen: svm: insufficiencies in handling emulated instructions during vm exits | bugzilla.redhat.com text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=702657 |
| access.redhat.com | web.archive.org text/html Inactive Link Not Archived | REDHAT RHSA-2011:1163 |
| access.redhat.com | web.archive.org text/html Inactive Link Not Archived | REDHAT RHSA-2011:1065 |
| oss-security - CVE-2011-1780, CVE-2011-1936, kernel/xen issues | www.openwall.com text/html | MLIST [oss-security] 20110707 CVE-2011-1780, CVE-2011-1936, kernel/xen issues |

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 | Xen | Xen | 3.0.3 | All | All | All |
| Operating System | Xen | Xen | 3.0.3 | All | All | All |

cpe:2.3:o:xen:xen:3.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.0.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→