CVE-2011-2901

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-2901
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-01 17:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Off-by-one error in the __addr_ok macro in Xen 3.3 and earlier allows local 64 bit PV guest administrators to cause a denia

Risk And Classification

Primary CVSS: v2.0 5.5 from nvd@nist.gov

AV:A/AC:L/Au:S/C:N/I:N/A:C

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Complete

AV:A/AC:L/Au:S/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	3.0.2	All	All	All

Operating System	Xen	Xen	3.0.3	All	All	All
Operating System	Xen	Xen	3.0.4	All	All	All
Operating System	Xen	Xen	3.1.3	All	All	All
Operating System	Xen	Xen	3.1.4	All	All	All
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	All	All	All
Operating System	Xen	Xen	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da2661108
728042 – (CVE-2011-2901) CVE-2011-2901 kernel: xen: off-by-one shift in x86_64 __addr_ok()	af854a3a-2127-422b-91ae-364da2661108
access.redhat.com	af854a3a-2127-422b-91ae-364da2661108
Security Advisory SA55082 - Gentoo update for xen - Secunia	af854a3a-2127-422b-91ae-364da2661108
oss-security - Xen Security Advisory 4 (CVE-2011-2901) - Xen 3.3 vaddr validation	af854a3a-2127-422b-91ae-364da2661108
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
access.redhat.com | CVE-2011-2901	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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