



CVE-2013-0190

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-0190
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-13 01:55:00 UTC
Updated	2013-03-08 04:11:00 UTC
Description	The xen_failsafe_callback function in Xen for the Linux kernel 2.6.23 and other versions, when running a 32-bit PVOPS gue

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source
USN-1728-1: Linux kernel (EC2) vulnerability Ubuntu	UBUNTU
Xen 'xen_failsafe_callback()' Function Local Denial of Service Vulnerability	BID
USN-1725-1: Linux kernel vulnerability Ubuntu	UBUNTU
Red Hat Customer Portal	REDHAT
oss-security - [PATCH] xen: Fix stack corruption in xen_failsafe_callback for 32bit PVOPS guests.	MLIST
oss-security - Xen Security Advisory 40 (CVE-2013-0190) - Linux stack corruption in xen_failsafe_callback for 32bit PVOPS guests.	MLIST
Bug 896038 – CVE-2013-0190 kernel: stack corruption in xen_failsafe_callback()	CONFIRMED
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)