



CVE-2014-2580

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

Summary

CVE	CVE-2014-2580
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-15 23:13:00 UTC
Updated	2014-04-16 13:57:00 UTC
Description	The netback driver in Xen, when using certain Linux versions that do not allow sleeping in softirq context, allows local guests to cause a denial of service.

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
XSA-90 - Xen Security Advisories	CO
Xen Netback Packet Processing Flaw Lets Local Guest Administrators Cause Denial of Service Conditions on the Host - SecurityTracker	SE
Xen Linux netback CVE-2014-2580 Remote Denial of Service Vulnerability	BI
oss-security - Xen Security Advisory 90 - Linux netback crash trying to disable due to malformed packet	MI
oss-security - Re: Xen Security Advisory 90 - Linux netback crash trying to disable due to malformed packet	MI
CVE Program record	CV
NVD vulnerability detail	NV

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](#)