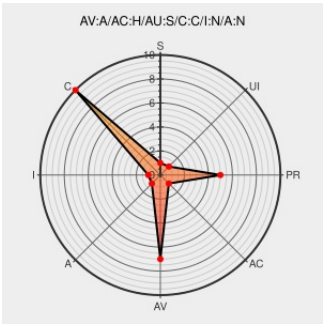
CVE-2013-2076

Published on: 08/28/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:28:00 AM UTC

CVE-2013-2076

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



Certain versions of Xen from Xen contain the following vulnerability:

Xen 4.0.x, 4.1.x, and 4.2.x, when running on AMD64 processors, only save/restore the FOP, FIP, and FDP x87 registers in FXSAVE/FXRSTOR when an exception is pending, which allows one domain to determine portions of the state of floating point instructions of other domains, which can be leveraged to obtain sensitive information such as cryptographic keys, a similar vulnerability to CVE-2006-1056. NOTE: this is the documented behavior of AMD64 processors, but it is inconsistent with Intel processors in a security-relevant fashion that was not addressed by the kernels.

CVE-2013-2076 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	NONE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3006-1 xen	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3006
Security Advisory SA55082 - Gentoo update for xen - Secunia	web.archive.org, text/html	SECUNIA 55082
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	security.gentoo.org, text/html	GENTOO GLSA-201309-24
oss-security - Xen Security Advisory 52 (CVE-2013-2076) - Information leak on XSAVE/XRSTOR capable AMD	www.openwall.com, text/html	MLIST [oss-security] 20130603 Xen Security Advisory 52 (CVE-2013-2076) - Information leak on

CPUs		XSAVE/XRSTOR capable AMD CPUs
[security-announce] SUSE-SU-2014:0446-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2014:0446

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	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating	Xen	Xen	4.0.2	All	All	All

System						
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All

cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.0.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.0.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.0.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.0.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.1.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.1.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.1.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.1.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.1.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.1.5:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.2.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.2.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.2.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→