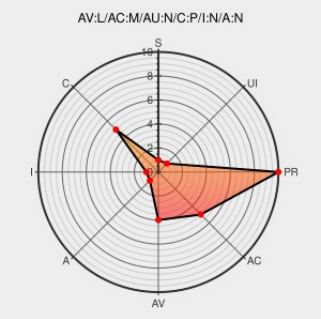
CVE-2013-4368

Published on: 10/17/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:14 AM UTC

CVE-2013-4368

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



Certain versions of Xen from Xen contain the following vulnerability:

The outs instruction emulation in Xen 3.1.x, 4.2.x, 4.3.x, and earlier, when using FS: or GS: segment override, uses an uninitialized variable as a segment base, which allows local 64-bit PV guests to obtain sensitive information (hypervisor stack content) via unspecified vectors related to stale data in a segment register.

CVE-2013-4368 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
oss-security - Xen Security Advisory 67 (CVE-2013-4368) - Information leak through outs instruction emulation	www.openwall.com, text/html	MLIST [oss-security] 20131010 Xen Security Advisory 67 (CVE-2013-4368) - Information leak through outs instruction emulation
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:1449
Debian -- Security Information -- DSA-3006-1 xen	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3006
[security-announce] SUSE-SU-2014:0411-1: important: Security update for	lists.opensuse.org, text/html	SUSE SUSE-SU-2014:0411
openSUSE-SU-2013:1636-1: moderate: xen: security and bugfix update to 4.	lists.opensuse.org, text/html	SUSE openSUSE-SU-2013:1636

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF xen-cve20134368-info-disc(87799)
Gentoo Linux Documentation -- Xen: Multiple Vunlerabilities	security.gentoo.org text/html	GENTOO GLSA-201407-03
[security-announce] SUSE-SU-2014:0470-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2014:0470
[security-announce] SUSE-SU-2014:0446-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2014:0446

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	3.0.2	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	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All

System						
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
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	4.1.6.1	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	4.2.3	All	All	All
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

System						
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	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
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	Xen	Xen	4.1.4	All	All	All

System						
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	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	4.2.3	All	All	All
Operating System	Xen	Xen	All	All	All	All

cpe:2.3:o:xen:xen:3.0.2:*:*:*:*:*:*:*

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

cpe:2.3:o:xen:xen:3.0.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.1.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.1.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.2.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.2.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.2.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.2.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.3.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.3.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.3.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.4:*:*:*:*:*:*:*

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:4.1.6.1:*:*:*:*:*:*:*:

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:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.0.2:*:*:*:*:*:*:*:

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

cpe:2.3:o:xen:xen:3.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.4:*:*:*:*:*:*:*:

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:4.1.6.1:*:*:*:*:*:*:*:

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:4.2.3:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→