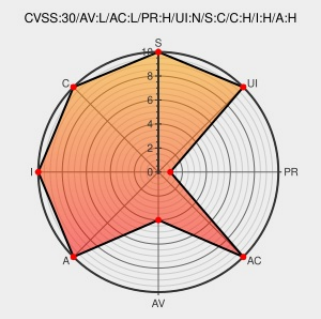
CVE-2015-8550

Published on: 04/14/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8550

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



Certain versions of Suse Linux Enterprise Real Time Extension from Novell contain the following vulnerability:

Xen, when used on a system providing PV backends, allows local guest OS administrators to cause a denial of service (host OS crash) or gain privileges by writing to memory shared between the frontend and backend, aka a double fetch vulnerability.

CVE-2015-8550 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5.7 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
Xen PV Backend Driver CVE-2015-8550 Remote Code Execution Vulnerability	Third Party Advisory, VDB Entry, cve.report (archive), text/html	BID 79592

Debian -- Security Information -- DSA-3471-1 qemu	www.debian.org Depreciated Link text/html	DEBIAN DSA-3471
Debian -- Security Information -- DSA-3434-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3434
Xen PV Backend Drivers Memory Double-Fetch Lets Local Administrative Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1034479
Debian -- Security Information -- DSA-3519-1 xen	www.debian.org Depreciated Link text/html	DEBIAN DSA-3519
Oracle VM Server for x86 Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
[security-announce] SUSE-SU-2016:1102-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1102
XSA-155 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-155.html
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201604-03
[security-announce] SUSE-SU-2016:1764-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:1764
[security-announce] SUSE-SU-2016:0911-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0911

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Real Time Extension	12	sp1	All	All
Operating System	Xen	Xen	-	All	All	All
Operating System	Xen	Xen	-	All	All	All

cpe:2.3:o:novell:suse_linux_enterprise_real_time_extension:12:sp1:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_real_time_extension:12:sp1:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_real_time_extension:12:sp1:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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