CVE-2015-5200

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-5200
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-08 15:59:00 UTC
Updated	2016-12-22 02:59:00 UTC
Description	The trace functionality in libvdpau before 1.1.1, when used in a setuid or setgid application, allows local users to write to arb

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Application	Libvdpau Project	Libvdpau	All	All	All	All

References

Reference	Source	Link	Tags
openSUSE-SU-2015:1537-1: moderate: Security update for libvdpau	SUSE	lists.opensuse.org	
libvdpau 1.1.1	MLIST	lists.x.org	
[SECURITY] Fedora 22 Update: libvdpau-1.1.1-1.fc22	FEDORA	lists.fedoraproject.org	
Bug 1253827 – CVE-2015-5200 libvdpau vulnerability in trace functionality	CONFIRM	bugzilla.redhat.com	
[SECURITY] Fedora 23 Update: libvdpau-1.1.1-1.fc23	FEDORA	lists.fedoraproject.org	
USN-2729-1: libvdpau vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com	
Debian -- Security Information -- DSA-3355-1 libvdpau	DEBIAN	www.debian.org	

libvdpau Multiple Local Security Vulnerabilities	BID	www.securityfocus.com	
[SECURITY] Fedora 21 Update: libvdpau-1.1.1-2.fc21	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.