CVE-2019-11085

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

Summary

CVE	CVE-2019-11085
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-17 16:29:00 UTC
Updated	2019-05-31 12:29:00 UTC
Description	Insufficient input validation in Kernel Mode Driver in Intel(R) i915 Graphics for Linux before version 5.0 may allow an auther

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Intel	I915	-	All	All	All
Hardware	Intel	I915	-	All	All	All
Operating System	Intel	I915 Firmware	All	All	All	All
Operating System	Intel	I915 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[security-announce] openSUSE-SU-2019:1479-1: important: Security update	SUSE	lists.opensuse.org	
Linux Kernel CVE-2019-11085 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com	
support.f5.com/csp/article/K09376613	CONFIRM	support.f5.com	Third Party Advis
INTEL-SA-00249	MISC	www.intel.com	Patch, Vendor Ac
Red Hat Customer Portal	REDHAT	access.redhat.com	
USN-4118-1: Linux kernel (AWS) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	

Red Hat Customer Portal	REDHAT	access.redhat.com	
USN-4068-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[security-announce] openSUSE-SU-2019:1579-1: important: Security update	SUSE	lists.opensuse.org	
USN-4068-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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