



CVE-2019-0136

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-0136
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-13 16:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Insufficient access control in the Intel(R) PROSet/Wireless WiFi Software driver before version 21.10 may allow an unauth

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Chrome Os	-	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Application	Intel	Proset/wireless Wifi	All	All	All	All
Application	Intel	Proset/wireless Wifi	All	All	All	All
Application	Intel	Proset/wireless Wifi	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All

References

Reference	Source	Link	Tags
Page Not Found - Lenovo Support US	CONFIRM	support.lenovo.com	Third Part

[SECURITY] [DLA 1930-1] linux security update	MLIST	lists.debian.org	
Malformed Request	BID	www.securityfocus.com	Third Part
[SECURITY] [DLA 2114-1] linux-4.9 security update	MLIST	lists.debian.org	
USN-4118-1: Linux kernel (AWS) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
INTEL-SA-00232	CONFIRM	www.intel.com	
USN-4115-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[SECURITY] [DLA 1919-2] linux-4.9 security update	MLIST	lists.debian.org	
Kernel Live Patch Security Notice LSN-0058-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
[SECURITY] [DLA 1919-1] linux-4.9 security update	MLIST	lists.debian.org	
USN-4147-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
JVN#75617741: Intel Dual Band Wireless-AC 8260 vulnerable to denial-of-service (DoS)	JVN	jvn.jp	
USN-4145-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [671064](#) EulerOS Security Update for kernel (EulerOS-SA-2019-2599)
- [751684](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 41 for SLE 12 SP3) (SUSE-SU-2022:0329-1)
- [751687](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 12 SP3) (SUSE-SU-2022:0328-1)
- [751688](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 12 SP3) (SUSE-SU-2022:0325-1)
- [751689](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 39 for SLE 12 SP3) (SUSE-SU-2022:0327-1)
- [751698](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0362-1)
- [753441](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:14905-1)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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