



# CVE-2021-0071

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

## Summary

<b>CVE</b>	CVE-2021-0071
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@intel.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-17 20:15:00 UTC
<b>Updated</b>	2021-11-21 14:50:00 UTC
<b>Description</b>	Improper input validation in firmware for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Intel</a>	7265	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">7265 Firmware</a>	All	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">9260 Firmware</a>	-	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 3165</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 3165 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 3168</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 3168 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 8260</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 8260 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 8265</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 8265 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 9260</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 9260 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 9461</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 9461 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ac 9462</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 9462 Firmware</a>	All	All	All	All

Hardware	<a href="#">Intel</a>	<a href="#">Ac 9560</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ac 9560 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ax200</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ax200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ax201</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ax201 Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Ax210</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Ax210 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
INTEL-SA-00509	MISC	<a href="http://www.intel.com">www.intel.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">751959</a> OpenSUSE Security Update for kernel-firmware (openSUSE-SU-2022:1065-1)
<a href="#">752007</a> SUSE Enterprise Linux Security Update for kernel-firmware (SUSE-SU-2022:1065-1)
<a href="#">752158</a> SUSE Enterprise Linux Security Update for kernel-firmware (SUSE-SU-2022:1751-1)

© [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](#)