



# CVE-2019-0149

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

## Summary

<b>CVE</b>	CVE-2019-0149
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@intel.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-14 19:15:00 UTC
<b>Updated</b>	2021-05-03 17:22:00 UTC
<b>Description</b>	Insufficient input validation in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an at

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intel	<a href="#">Ethernet 700 Series Software</a>	All	All	All	All
Application	Intel	<a href="#">Ethernet 700 Series Software</a>	All	All	All	All
Application	Intel	<a href="#">Ethernet 700 Series Software</a>	All	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller 710-bm1</a>	-	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller 710-bm1</a>	-	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller 710-bm1 Firmware</a>	All	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller 710-bm1 Firmware</a>	All	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller X710-at2</a>	-	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller X710-at2</a>	-	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller X710-at2 Firmware</a>	All	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller X710-at2 Firmware</a>	All	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller X710-bm2</a>	-	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller X710-bm2</a>	-	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller X710-bm2 Firmware</a>	All	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller X710-bm2 Firmware</a>	All	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller X710-tm4</a>	-	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller X710-tm4</a>	-	All	All	All

Operating System	Intel	<a href="#">Ethernet Controller X710-tm4 Firmware</a>	All	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller X710-tm4 Firmware</a>	All	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller Xxv710-am1</a>	-	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller Xxv710-am1</a>	-	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller Xxv710-am1 Firmware</a>	All	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller Xxv710-am1 Firmware</a>	All	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller Xxv710-am2</a>	-	All	All	All
Hardware	Intel	<a href="#">Ethernet Controller Xxv710-am2</a>	-	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller Xxv710-am2 Firmware</a>	All	All	All	All
Operating System	Intel	<a href="#">Ethernet Controller Xxv710-am2 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
INTEL-SA-00255	MISC	<a href="http://www.intel.com">www.intel.com</a>	Patch, Vendor Advisory
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

[672410](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2796)

[672474](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2823)

© [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](https://status.cve.report)