



CVE-2021-0004

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

Summary

CVE	CVE-2021-0004
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-11 13:15:00 UTC
Updated	2023-11-07 03:27:00 UTC
Description	Improper buffer restrictions in the firmware of Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters be

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Hardware	Intel	Ethernet Controller E810	-	All	All	All
Operating System	Intel	Ethernet Controller E810 Firmware	All	All	All	All

References

Reference	Source	Link	Tag
INTEL-SA-00479	MISC	www.intel.com	
Intel SA-00479 Ethernet Controller Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] Fedora 34 Update: nodejs-14.18.3-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: nodejs-14.18.3-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)