CVE-2008-2476

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

Summary

CVE	CVE-2008-2476
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-03 15:07:00 UTC
Updated	2017-09-29 01:31:00 UTC
Description	The IPv6 Neighbor Discovery Protocol (NDP) implementation in (1) FreeBSD 6.3 through 7.1, (2) OpenBSD 4.2 and 4.3, (3

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Force10	Ftos	All	All	All	All
Operating System	Force10	Ftos	All	All	All	All
Operating System	Freebsd	Freebsd	6.3	All	All	All
Operating System	Freebsd	Freebsd	7.1	All	All	All
Operating System	Freebsd	Freebsd	6.3	All	All	All
Operating System	Freebsd	Freebsd	7.1	All	All	All
Operating System	Juniper	Jnos	All	All	All	All
Operating System	Juniper	Jnos	All	All	All	All
Operating System	Netbsd	Netbsd	All	All	All	All
Operating System	Netbsd	Netbsd	All	All	All	All
Operating System	Openbsd	Openbsd	4.2	All	All	All
Operating System	Openbsd	Openbsd	4.3	All	All	All
Operating System	Openbsd	Openbsd	4.2	All	All	All
Operating System	Openbsd	Openbsd	4.3	All	All	All
Operating System	Windriver	Vxworks	5	All	All	All
Operating System	Windriver	Vxworks	5.5	All	All	All
Operating System	Windriver	Vxworks	5	All	All	All

Operating System	Windriver	Vxworks	5.5	All	All	All
Operating System	Windriver	Vxworks	All	All	All	All

References

Reference
OpenBSD 4.3 errata
OpenBSD IPv6 Neighbor Discovery Protocol Spoofing Bug Lets Remote Users Modify Routing Data in Certain Cases - SecurityTracker
Juniper Networks
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
OpenBSD 4.2 errata
IBM X-Force Exchange
Juniper Products Neighbor Discovery Protocol Neighbor Solicitation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.co
Force10 FTOS Routers IPv6 Neighbor Discovery Protocol Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
FreeBSD IPv6 Neighbor Discovery Protocol Neighbor Solicitation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Force10 Networks, Inc. Information for VU#472363
OpenBSD IPv6 Neighbor Discovery Protocol Neighbor Solicitation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com
NetBSD-SA2008-013
US-CERT Vulnerability Note VU#472363
NetBSD IPv6 Neighbor Discovery Protocol Spoofing Bug Lets Remote Users Modify Routing Data in Certain Cases - SecurityTracker
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecurityTracker.com Archives - FreeBSD IPv6 Neighbor Discovery Protocol Spoofing Bug Lets Remote Users Modify Routing Data in Certain
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
NetBSD IPv6 Neighbor Discovery Protocol Neighbor Solicitation Vulnerability - Secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
FreeBSD-SA-08:10
Multiple Vendors IPv6 Neighbor Discovery Protocol Implementation Address Spoofing Vulnerability
Wind River Systems, Inc. Information for VU#472363
Repository / Oval Repository
About the security content of Time Capsule and AirPort Base Station (802.11n*) Firmware 7.4.1
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2017-09-28	Joshua Bressers	Not vulnerable. This issue did not affect the versions of Linux kernel as shipped with Red Ha

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 registred 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**