



CVE-2014-3554

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

Summary

CVE	CVE-2014-3554
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-31 14:55:00 UTC
Updated	2021-10-12 14:28:00 UTC
Description	Buffer overflow in the ndp_msg_opt_dnssl_domain function in libndp allows remote routers to cause a denial of service (crash) by sending a crafted packet to the router. The vulnerability exists in the ndp_msg_opt_dnssl_domain function in libndp. The function does not properly validate the length of the input data, which can lead to a buffer overflow and a denial of service (crash). The vulnerability is present in libndp versions 1.10 and earlier.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libndp	Libndp	All	All	All	All
Application	Libndp	Libndp	-	All	All	All
Application	Libndp	Libndp	-	All	All	All

References

Reference	Source	Link
oss-security - CVE-2014-3554: libndp buffer overflow	MLIST	www.openwall.com
Bug 1118583 – CVE-2014-3554 libndp: buffer overflow flaw in DNS Search List (DNSSL) handling	CONFIRM	bugzilla.redhat.com
libndp 'ndp_msg_opt_dnssl_domain()' Function Buffer Overflow Vulnerability	BID	www.securityfocus.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

671060 EulerOS Security Update for libndp (EulerOS-SA-2019-2611)

© [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](#)