



CVE-2019-6472

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

Summary

CVE	CVE-2019-6472
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-16 18:15:00 UTC
Updated	2019-12-05 14:28:00 UTC
Description	A packet containing a malformed DUID can cause the Kea DHCPv6 server process (kea-dhcp6) to exit due to an assertion

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Kea	1.6.0	beta1	All	All
Application	isc	Kea	1.6.0	beta2	All	All
Application	isc	Kea	1.6.0	beta1	All	All
Application	isc	Kea	1.6.0	beta2	All	All
Application	isc	Kea	All	All	All	All

References

Reference	Source	Link
CVE-2019-6472: A packet containing a malformed DUID can cause the kea-dhcp6 server to terminate - Security Advisories	CONFIRM	kb...
CVE Program record	CVE.ORG	ww...
NVD vulnerability detail	NVD	nv...

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501024](#) Alpine Linux Security Update for kea

[504037](#) Alpine Linux Security Update for kea

© [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](#)