



CVE-2019-6475

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-6475
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-17 20:15:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	Mirror zones are a BIND feature allowing recursive servers to pre-cache zone data provided by other servers. A mirror zone

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Bind	All	All	All	All
Application	isc	Bind	All	All	All	All

References

Reference	Source	Link
October 2019 ISC BIND Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netap
CVE-2019-6475: A flaw in mirror zone validity checking can allow zone data to be spoofed - Security Advisories	CONFIRM	kb.isc.org
myF5		support.f5.com
support.f5.com/csp/article/K42238532	CONFIRM	support.f5.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

[500056](#) Alpine Linux Security Update for bind

[503737](#) Alpine Linux Security Update for bind

© [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](#)