



CVE-2016-6271

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

Summary

CVE	CVE-2016-6271
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-18 22:59:00 UTC
Updated	2017-08-03 01:29:00 UTC
Description	The Bzrtp library (aka libbzrtp) 1.0.x before 1.0.4 allows man-in-the-middle attackers to conduct spoofing attacks by leverag

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bzrtp Project	Bzrtp	1.0.0	All	All	All
Application	Bzrtp Project	Bzrtp	1.0.2	All	All	All
Application	Bzrtp Project	Bzrtp	1.0.3	All	All	All
Application	Bzrtp Project	Bzrtp	1.0.0	All	All	All
Application	Bzrtp Project	Bzrtp	1.0.2	All	All	All
Application	Bzrtp Project	Bzrtp	1.0.3	All	All	All

References

Reference	Source	Link
Bzrtp CVE-2016-6271 Man in the Middle Spoofing Vulnerability	BID	www
GitHub - gteissier/CVE-2016-6271: Proof of concept for ZRTP man-in-the-middle	MISC	gith
Add ZRTP Commit packet hvi check on DHPart2 packet reception · BelledonneCommunications/bzrtp@bbb1e6e · GitHub	CONFIRM	gith
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

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](#)