



CVE-2020-7466

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

Summary

CVE	CVE-2020-7466
State	PUBLIC
Assigner	secteam@freebsd.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-06 14:15:00 UTC
Updated	2023-07-19 00:56:00 UTC
Description	The PPP implementation of MPD before 5.9 allows a remote attacker who can send specifically crafted PPP authentication

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mpd Project	Mpd	All	All	All	All
Application	Mpd Project	Mpd	All	All	All	All
Application	Stormshield	Stormshield Network Security	All	All	All	All
Application	Stormshield	Stormshield Network Security	4.4.0	All	All	All

References

Reference	Source	Link	Tags
MPD: FreeBSD PPP daemon / Bugs / #69 report a vulnerability	MISC	sourceforge.net	Exploit, Third Party Advisory
MPD: FreeBSD PPP daemon / Code / Commit [r2374]	MISC	sourceforge.net	Patch, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[690543](#) Free Berkeley Software Distribution (FreeBSD) Security Update for multi-link ppp protocol daemon mpd5 remotely exploitable crash (cd97c7ca-f079-11ea-9c31-001b216d295b)

© [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](#)