



CVE-2023-30367

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

Summary

CVE	CVE-2023-30367
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-26 21:15:00 UTC
Updated	2023-08-04 14:53:00 UTC
Description	Multi-Remote Next Generation Connection Manager (mRemoteNG) is free software that enables users to store and manage

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mremoteng	Mremoteng	1.77.2-nb	All	All	All
Application	Mremoteng	Mremoteng	1.77.3-nb	All	All	All
Application	Mremoteng	Mremoteng	All	All	All	All

References

Reference	Source	Link
mRemoteNG 1.77.3.1784-NB Sensitive Information Extraction ≈ Packet Storm	MISC	packetstormsecurity.com
Public Disclosure of issue 726 · Issue #2420 · mRemoteNG/mRemoteNG · GitHub	MISC	github.com
www.secuvera.de/advisories/secuvera-SA-2023-01.txt	MISC	www.secuvera.de
GitHub - S1lkys/CVE-2023-30367-mRemoteNG-password-dumper: Original PoC for CVE-2023-30367	MISC	github.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

[379270](#) Multi-Remote Next Generation Connection Manager (mRemoteNG) Password Dumper Vulnerability

© [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](#)