



CVE-2019-1000023

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

Summary

CVE	CVE-2019-1000023
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-04 21:29:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	OPT/NET BV OPTOSS Next Gen Network Management System (NG-NetMS) version v3.6-2 and earlier versions contains :

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opt-net	Ng-netms	All	All	All	All

References

Reference	Source	Link	Tags
OPTOSS NG-NetMS SourceForge.net	MISC	sourceforge.net	Prod
Site not found · GitHub Pages		inf0seq.github.io	
SQL Injection in OPTOSS Next Gen Network Management System (NG-NetMS) - Information security	MISC	inf0seq.github.io	Expl
SQL injection - OWASP	MISC	www.owasp.org	Thirc
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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