



CVE-2021-39168

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

Summary

CVE	CVE-2021-39168
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-27 00:15:00 UTC
Updated	2021-09-01 17:11:00 UTC
Description	OpenZeppelin is a library for smart contract development. In affected versions a vulnerability in TimelockController allowed a

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openzeppelin	Contracts	All	All	All	All

References

Reference	Source
TimelockController vulnerability in OpenZeppelin Contracts · Advisory · OpenZeppelin/openzeppelin-contracts-upgradeable · GitHub	CONF
openzeppelin-contracts/CHANGELOG.md at master · OpenZeppelin/openzeppelin-contracts · GitHub	MISC
Add additional isOperationReady check in TimelockController · OpenZeppelin/openzeppelin-contracts@cec4f2e · GitHub	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981059](#) Nodejs (npm) Security Update for @openzeppelin/contracts-upgradeable (GHSA-vrw4-w73r-6mm8)

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