



CVE-2020-20178

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

Summary

CVE	CVE-2020-20178
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-24 19:15:00 UTC
Updated	2021-09-20 12:15:00 UTC
Description	Ethereum 0xe933c0cd9784414d5f278c114904f5a84b396919#code.sol latest version is affected by a denial of service vuln

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openldap	Openldap	-	All	All	All
Application	Redhat	Ansible	All	All	All	All
Application	Whohas Project	Whohas	-	All	All	All

References

Reference	Source	Link	Tags
CVE-2020-20178 OpenLDAP Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
1914774 – (CVE-2021-20178) CVE-2021-20178 ansible: user data leak in snmp_facts module	MISC	bugzilla.redhat.com	
Attention Required! Cloudflare	MISC	etherscan.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[900111](#) CBL-Mariner Linux Security Update for ansible 2.9.12

[902845](#) Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (4240)

© [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](#)