CVE-2020-8172

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8172
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-08 14:15:00 UTC
Updated	2022-05-12 15:01:00 UTC
Description	TLS session reuse can lead to host certificate verification bypass in node version < 12.18.0 and < 14.4.0.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Oracle	Banking Extensibility Workbench	14.3.0	All	All	All
Application	Oracle	Banking Extensibility Workbench	14.4.0	All	All	All
Application	Oracle	Blockchain Platform	All	All	All	All
Application	Oracle	Graalvm	19.3.2	All	All	All
Application	Oracle	Graalvm	20.1.0	All	All	All
Application	Oracle	Mysql Cluster	All	All	All	All
Application	Oracle	Mysql Cluster	All	All	All	All
Application	Oracle	Mysql Cluster	All	All	All	All
Application	Oracle	Mysql Cluster	All	All	All	All
Application	Oracle	Mysql Cluster	All	All	All	All

References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - July 2020	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
June 2020 Security Releases | Node.js	MISC	nodejs.org	Vendor Advisory

June 2020 Security Releases | Node.js	MISC	nodejs.org	Vendor Advisory
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
CVE-2020-8172 Nodejs Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
HackerOne	MISC	hackerone.com	Exploit, Third Party
NodeJS: Multiple vulnerabilities (GLSA 202101-07) — Gentoo security	GENTOO	security.gentoo.org	
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com	
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

- 375444 IBM Spectrum Control Node js Vulnerability(6261327)
- 500436 Alpine Linux Security Update for nodejs
- 501097 Alpine Linux Security Update for nodejs-current
- 501444 Alpine Linux Security Update for nodejs
- 504199 Alpine Linux Security Update for nodejs
- 940104 AlmaLinux Security Update for nodejs:12 (ALSA-2020:2852)