



# CVE-2020-7712

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

## Summary

<b>CVE</b>	CVE-2020-7712
<b>State</b>	PUBLIC
<b>Assigner</b>	report@snyk.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-08-30 08:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	This affects the package json before 10.0.0. It is possible to inject arbitrary commands using the parseLookup function.

## Risk And Classification

**Problem Types:** CWE-78

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joyent	Json	All	All	All	All
Application	Joyent	Json	All	All	All	All
Application	Oracle	Commerce Guided Search	11.3.2	All	All	All
Application	Oracle	Financial Services Crime And Compliance Management Studio	8.0.8.2.0	All	All	All
Application	Oracle	Financial Services Crime And Compliance Management Studio	8.0.8.3.0	All	All	All
Application	Oracle	Financial Services Regulatory Reporting With Agilereporter	8.0.9.6.3	All	All	All
Application	Oracle	Timesten In-memory Database	All	All	All	All

## References

Reference	Source
Invalid vulnerability	MISC
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	MLIST
Command Injection in org.wahere.permissions   Snyk	MISC



## Legacy QID Mappings

982663 Nodejs (npm) Security Update for json (GHSA-3c6g-pvg8-gqw2)

© [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](#)