



CVE-2020-8203

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-8203 |
| State | PUBLIC |
| Assigner | support@hackerone.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-07-15 17:15:00 UTC |
| Updated | 2024-01-21 02:37:00 UTC |
| Description | Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20. |

Risk And Classification

Problem Types: CWE-1321

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------|--|---------|--------|---------|----------|
| Application | Lodash | Lodash | All | All | All | All |
| Application | Lodash | Lodash | All | All | All | All |
| Application | Oracle | Banking Corporate Lending Process Management | 14.2.0 | All | All | All |
| Application | Oracle | Banking Corporate Lending Process Management | 14.3.0 | All | All | All |
| Application | Oracle | Banking Corporate Lending Process Management | 14.5.0 | All | All | All |
| Application | Oracle | Banking Credit Facilities Process Management | 14.2.0 | All | All | All |
| Application | Oracle | Banking Credit Facilities Process Management | 14.3.0 | All | All | All |
| Application | Oracle | Banking Credit Facilities Process Management | 14.5.0 | All | All | All |
| Application | Oracle | Banking Extensibility Workbench | 14.2.0 | All | All | All |
| Application | Oracle | Banking Extensibility Workbench | 14.3.0 | All | All | All |
| Application | Oracle | Banking Extensibility Workbench | 14.5.0 | All | All | All |
| Application | Oracle | Banking Liquidity Management | 14.2.0 | All | All | All |
| Application | Oracle | Banking Liquidity Management | 14.3.0 | All | All | All |
| Application | Oracle | Banking Liquidity Management | 14.5.0 | All | All | All |
| Application | Oracle | Banking Supply Chain Finance | 14.2.0 | All | All | All |
| Application | Oracle | Banking Supply Chain Finance | 14.3.0 | All | All | All |
| Application | Oracle | Banking Supply Chain Finance | 14.5.0 | All | All | All |

| | | | | | | |
|-------------|--------|---|------------|-----|-----|-----|
| Application | Oracle | Banking Trade Finance Process Management | 14.2.0 | All | All | All |
| Application | Oracle | Banking Trade Finance Process Management | 14.3.0 | All | All | All |
| Application | Oracle | Banking Trade Finance Process Management | 14.5.0 | All | All | All |
| Application | Oracle | Banking Virtual Account Management | 14.2.0 | All | All | All |
| Application | Oracle | Banking Virtual Account Management | 14.3.0 | All | All | All |
| Application | Oracle | Banking Virtual Account Management | 14.5.0 | All | All | All |
| Application | Oracle | Blockchain Platform | All | All | All | All |
| Application | Oracle | Communications Billing And Revenue Management | 12.0.0.3.0 | All | All | All |
| Application | Oracle | Communications Billing And Revenue Management | 7.5.0.23.0 | All | All | All |
| Application | Oracle | Communications Cloud Native Core Policy | 1.11.0 | All | All | All |
| Application | Oracle | Communications Session Border Controller | 8.4 | All | All | All |
| Application | Oracle | Communications Session Border Controller | 9.0 | All | All | All |
| Application | Oracle | Communications Session Border Controller | cz8.4 | All | All | All |
| Application | Oracle | Communications Session Router | cz8.4 | All | All | All |
| Application | Oracle | Communications Subscriber-aware Load Balancer | cz8.3 | All | All | All |
| Application | Oracle | Communications Subscriber-aware Load Balancer | cz8.4 | All | All | All |
| Application | Oracle | Enterprise Communications Broker | 3.2.0 | All | All | All |
| Application | Oracle | Enterprise Communications Broker | 3.3.0 | All | All | All |
| Application | Oracle | Enterprise Communications Broker | pcz3.3 | All | All | All |
| Application | Oracle | Jd Edwards Enterpriseone Tools | All | All | All | All |
| Application | Oracle | Peoplesoft Enterprise Peopletools | 8.58 | All | All | All |
| Application | Oracle | Peoplesoft Enterprise Peopletools | 8.59 | All | All | All |
| Application | Oracle | Primavera Gateway | All | All | All | All |
| Application | Oracle | Primavera Gateway | All | All | All | All |
| Application | Oracle | Primavera Gateway | All | All | All | All |
| Application | Oracle | Primavera Gateway | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|-------------|
| CVE-2020-8203 Lodash Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | Third Part |
| Oracle Critical Patch Update Advisory - April 2022 | MISC | www.oracle.com | |
| CVE-2020-8203 is not modified in /.internal/baseSet.js · Issue #4874 · lodash/lodash · GitHub | MISC | github.com | Issue Tra |
| Oracle Critical Patch Update Advisory - July 2021 | N/A | www.oracle.com | |
| Oracle Critical Patch Update Advisory - October 2021 | MISC | www.oracle.com | |
| Oracle Critical Patch Update Advisory - January 2022 | MISC | www.oracle.com | |
| HackerOne | MISC | hackerone.com | Exploit, TI |

| | | | |
|--|---------|--|-----------|
| Oracle Critical Patch Update Advisory - April 2021 | MISC | www.oracle.com | |
| 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

[376257](#) Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUJAN2022)

[377843](#) Lodash Prototype Pollution Vulnerability

[378599](#) Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

[980321](#) Nodejs (npm) Security Update for lodash (GHSA-p6mc-m468-83gw)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report