



# CVE-2020-9281

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

## Summary

<b>CVE</b>	CVE-2020-9281
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-03-07 01:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	A cross-site scripting (XSS) vulnerability in the HTML Data Processor for CKEditor 4.0 before 4.14 allows remote attackers

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Ckeditor</a>	<a href="#">Ckeditor</a>	All	All	All	All
Application	<a href="#">Ckeditor</a>	<a href="#">Ckeditor</a>	All	All	All	All
Application	<a href="#">Drupal</a>	<a href="#">Drupal</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Plm</a>	9.3.5	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Plm</a>	9.3.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Product Lifecycle Management</a>	9.3.5	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Product Lifecycle Management</a>	9.3.6	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Application Express</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.10.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.12.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.6.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.7.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Management</a>	2.7.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Enterprise Default Managment</a>	2.10.0	All	All	All

Application	Oracle	Banking Enterprise Default Management	2.12.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.6.2	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.7.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.7.1	All	All	All
Application	Oracle	Banking Enterprise Default Management	All	All	All	All
Application	Oracle	Banking Platform	2.4.0	All	All	All
Application	Oracle	Banking Platform	2.7.0	All	All	All
Application	Oracle	Banking Platform	2.7.1	All	All	All
Application	Oracle	Banking Platform	2.8.0	All	All	All
Application	Oracle	Banking Platform	2.9.0	All	All	All
Application	Oracle	Commerce Merchandising	11.0.0	All	All	All
Application	Oracle	Commerce Merchandising	11.1.0	All	All	All
Application	Oracle	Commerce Merchandising	11.2.0	All	All	All
Application	Oracle	Commerce Merchandising	11.3.0	All	All	All
Application	Oracle	Commerce Merchandising	11.3.1	All	All	All
Application	Oracle	Commerce Merchandising	11.3.2	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	All	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	-	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Oracle	Siebel Apps - Customer Order Management	All	All	All	All
Application	Oracle	Siebel Customer Order Management	All	All	All	All
Application	Oracle	Webcenter Portal	11.1.1.9.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.4.0	All	All	All

## References

Reference	Source
[SECURITY] Fedora 32 Update: ckeditor-4.14.0-1.fc32 - package-announce - Fedora Mailing-Lists	
GitHub - ckeditor/ckeditor4: The best enterprise-grade WYSIWYG editor. Fully customizable with countless features and plugins.	MISC
[SECURITY] Fedora 30 Update: ckeditor-4.14.0-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
Oracle Critical Patch Update Advisory - October 2020	MISC
Oracle Critical Patch Update Advisory - October 2021	MISC
Oracle Critical Patch Update Advisory - January 2022	MISC
[SECURITY] Fedora 31 Update: ckeditor-4.14.0-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA

[SECURITY] Fedora 31 Update: ckeditor-4.14.0-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 30 Update: ckeditor-4.14.0-1.fc30 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 32 Update: ckeditor-4.14.0-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
Oracle Critical Patch Update Advisory - April 2021	MISC
Oracle Critical Patch Update Advisory - January 2021	MISC
[SECURITY] Fedora 31 Update: ckeditor-4.14.0-1.fc31 - package-announce - Fedora Mailing-Lists	
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[198710](#) Ubuntu Security Notification for CKEditor Vulnerabilities (USN-5340-1)

[374875](#) Oracle PeopleSoft Enterprise PeopleTools Multiple vulnerabilities (CPUJAN2021)

[980303](#) Nodejs (npm) Security Update for ckeditor4 (GHSA-vcjf-mgcg-jxjq)

© [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](#)**