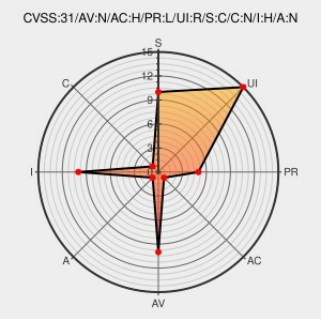
CVE-2020-26237

Published on: 11/24/2020 12:00:00 AM UTC

Last Modified on: 10/19/2022 01:49:00 PM UTC

CVE-2020-26237 - advisory for GHSA-vfrc-7r7c-w9mx

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

Highlight.js is a syntax highlighter written in JavaScript. Highlight.js versions before 9.18.2 and 10.1.2 are vulnerable to Prototype Pollution. A malicious HTML code block can be crafted that will result in prototype pollution of the base object's prototype during highlighting. If you allow users to insert custom HTML code blocks into your page/app via parsing Markdown code blocks (or similar) and do not filter the language names the user can provide you may be vulnerable. The pollution should just be harmless data but this can cause problems for applications not expecting these properties to exist and can result in strange behavior or application crashes, i.e. a potential DOS vector. If your website or application does not render user provided data it should be unaffected. Versions 9.18.2 and 10.1.2 and newer include fixes for this vulnerability. If you are using version 7 or 8 you are encouraged to upgrade to a newer release.

CVE-2020-26237 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **highlightjs** - **highlight.js** version **< 9.18.2**

Affected Vendor/Software: **highlightjs** - **highlight.js** version **>= 10.0.0, < 10.1.2**

CVSS3 Score: 8.7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	HIGH	HIGH

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
use null prototype objects for languages/aliases by night · Pull Request #2636 · highlightjs/highlight.js · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/highlightjs/highlight.js/pull/2636
[SECURITY] [DLA 2511-1] highlight.js security update	lists.debian.org, text/html	MLIST [debian-lts-announce] 20201230 [SECURITY] [DLA 2511-1] highlight.js se update
(parser) use null prototype objects for languages/aliases (#2636) · highlightjs/highlight.js@7241013 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/highlightjs/highlight.js/commit/7241013ae011a585983e176ddc0489a7a52
Prototype Pollution · Advisory · highlightjs/highlight.js · GitHub	Mitigation, Third Party Advisory, github.com, text/html	CONFIRM github.com/highlightjs/highlight.js/security/advisories/GHSA-vfrc-7r7c-v
Oracle Critical Patch Update Advisory - July 2022	www.oracle.com, text/html	MISC www.oracle.com/security-alerts/cpujul2022.html
highlight.js	Third Party Advisory, www.npmjs.com, text/html	MISC www.npmjs.com/package/highlight.js

Related QID Numbers

983099 Nodejs (npm) Security Update for highlight.js (GHSA-vfrc-7r7c-w9mx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Highlightjs	Highlight.js	All	All	All	All
Application	Highlightjs	Highlight.js	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

cpe:2.3:a:highlightjs:highlight.js:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:highlightjs:highlight.js:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:oracle:mysql_enterprise_monitor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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