



CVE-2020-15092

Published on: 07/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-15092 - advisory for GHSA-2jpm-827p-j44g

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Timelinejs](#) from [Northwestern](#) contain the following vulnerability:

In TimelineJS before version 3.7.0, some user data renders as HTML. An attacker could implement an XSS exploit with maliciously crafted content in a number of data fields. This risk is present whether the source data for the timeline is stored on Google Sheets or in a JSON configuration file. Most TimelineJS users configure their timeline with a

Google Sheets document. Those users are exposed to this vulnerability if they grant write access to the document to a malicious inside attacker, if the access of a trusted user is compromised, or if they grant public write access to the document. Some TimelineJS users configure their timeline with a JSON document. Those users are exposed to this vulnerability if they grant write access to the document to a malicious inside attacker, if the access of a trusted user is compromised, or if write access to the system hosting that document is otherwise compromised. Version 3.7.0 of TimelineJS addresses this in two ways. For content which is intended to support limited HTML markup for styling and linking, that content is "sanitized" before being added to the DOM. For content intended for simple text display, all markup is stripped. Very few users of TimelineJS actually install the TimelineJS code on their server. Most users publish a timeline using a URL hosted on systems we control. The fix for this issue is published to our system such that **those users will automatically begin using the new code**. The only exception would be users who have deliberately edited the embed URL to "pin" their timeline to an earlier version of the code. Some users of TimelineJS use it as a part of a wordpress plugin (knight-lab-timelinejs). Version 3.7.0.0 of that plugin and newer integrate the updated code. Users are encouraged to update the plugin rather than manually update the embedded version of TimelineJS.

CVE-2020-15092 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **NUKnightLab - TimelineJS3** version < 3.7.0

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Posts Knight Lab	Vendor Advisory knightlab.northwestern.edu text/html	◆ MISC knightlab.northwestern.edu/posts/
Stored XSS vulnerability when rendering data · Advisory · NUKnightLab/TimelineJS3 · GitHub	Patch Third Party Advisory github.com text/html	🔒 CONFIRM github.com/NUKnightLab/TimelineJS3/security/advisories/GHSA-2jpm-827p-j44g

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Northwestern	Timelinejs	All	All	All	All
Application	Northwestern	Timelinejs	All	All	All	All
cpe:2.3:a:northwestern:timelinejs:*:*:*:*:*:*:						
cpe:2.3:a:northwestern:timelinejs:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#)