



CVE-2018-1000086

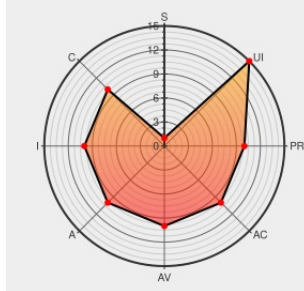
Published on: 03/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000086

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Pym.js](#) from [Npr](#) contain the following vulnerability: NPR Visuals Team Pym.js version versions 0.4.2 up to 1.3.1 contains a Cross site Request Forgery (CSRF) vulnerability in Pym.js `_onNavigateToMessage` function. <https://github.com/nprapps/pym.js/blob/master/src/pym.js#L573> that can result in Arbitrary javascript code execution. This attack appear to be exploitable via Attacker gains full javascript access to pages with Pym.js embeds when user visits an attacker crafted page.. This vulnerability appears to have been fixed in versions 1.3.2 and later.

CVE-2018-1000086 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Scripting vul. Issue #170 - nprapps/pym.js - GitHub	CVE-2018-1000086	MISC

Sanitize url · Issue #170 · nprapps/pym.js · GitHub	Third Party Advisory github.com text/html	 MISC github.com/nprapps/pym.js/issues/170
Pym.js Security Alert NPR Visuals	Vendor Advisory blog.apps.npr.org text/html	 MISC blog.apps.npr.org/2018/02/15/pym-security-vulnerability.html
GitHub - nprapps/pym.js: Resize an iframe responsively depending on the height of its content and the width of its container.	Product github.com text/html	 MISC github.com/nprapps/pym.js

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.

Related QID Numbers

981218 Nodejs (npm) Security Update for pym.js (GHSA-82gw-pqf7-q3j2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Npr	Pym.js	All	All	All	All
cpe:2.3:a:npr:pym.js:*:*:*:*:*:						

No vendor comments have been submitted for this CVE