CVE-2020-8116

Prototype pollution vulnerability in dot-prop npm package versions before 4.2.1 and versions 5.x before 5.1.1 allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.

CODE SCORING
Administrator
Dashboard
Policy alerts
Projects
Dependencies
Licenses
Vulnerabilities
Authors
Code clones
Settings
Log out

Published	Updated	Affected Projects	Weakness Type (CWE)
04.02.2020	10.09.2020	1	CWE-425

CVSS 2 Score	CVSS 3 Score
7.5 HIGH	7.3 HIGH

CVSS2 Metrics (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Access Vector (AV)
Local (L) | Adjacent Network (A) | **Network (N)**

Access Complexity (AC)
High (H) | Medium (M) | **Low (L)**

Authentication (Au)
Multiple (M) | Single (S) | **None (N)**

Confidentiality Impact (C)
None (N) | **Partial (P)** | Complete (C)

Integrity Impact (I)
None (N) | **Partial (P)** | Complete (C)

Availability Impact (A)
None (N) | **Partial (P)** | Complete (C)

CVSS3 Metrics (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Attack Vector (AV)
Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)
Low (L) | High (H)

Privileges Required (PR)
None (N) | Low (L) | High (H)

User Interaction (UI)
None (N) | Required (R)

Scope (S)
Unchanged (U) | Changed (C)

Confidentiality (C)
None (N) | **Low (L)** | High (H)

Integrity (I)
None (N) | **Low (L)** | High (H)

Availability (A)
None (N) | **Low (L)** | High (H)

Affected dependencies

Total 1 item

< 1 > 10 / page

Dependency	Project	Found
dot-prop@4.2.0	React	20.08.2021 11:50

Total 1 item

< 1 > 10 / page

References

Hyperlink	Resource
https://hackerone.com/reports/719856	Exploit, Third Party Advisory
https://github.com/sindresorhus/dot-prop/issues/63	
https://github.com/sindresorhus/dot-prop/tree/v4	
https://github.com/advisories/GHSA-ff7x-qrg7-qggm	