



# CVE-2020-13822

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-13822
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-04 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:16:00 UTC
<b>Description</b>	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading '\0' bytes, or i

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Elliptic Project</a>	<a href="#">Elliptic</a>	6.5.2	All	All	All
Application	<a href="#">Elliptic Project</a>	<a href="#">Elliptic</a>	6.5.2	All	All	All

## References

Reference	Source
<a href="#">elliptic</a>	MISC
<a href="#">Malleability-Attack: Why It Matters – Herman Schoenfeld – Medium</a>	MISC
<a href="#">How Not to Use ECDSA – Learning Words</a>	MISC
<a href="#">Lack of encoding checks allows a certain degree of signature malleability in ECDSA signatures · Issue #226 · indutny/elliptic · GitHub</a>	MISC
<a href="#">Malleability-Attack: Why It Matters   by Herman Schoenfeld   Medium</a>	
<a href="#">CVE Program record</a>	CVE.
<a href="#">NVD vulnerability detail</a>	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[378599](#) Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

© [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](#)