



CVE-2018-8319

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-8319
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-11 00:29:00 UTC
Updated	2018-09-05 12:19:00 UTC
Description	A Security Feature Bypass vulnerability exists in MSR JavaScript Cryptography Library that is caused by incorrect arithmetic

Risk And Classification

Problem Types: CWE-682

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Research Javascript Cryptography Library	1.4	All	All	All
Application	Microsoft	Research Javascript Cryptography Library	1.4	All	All	All

References

Reference

- Microsoft MSR JavaScript Cryptography Library CVE-2018-8319 Remote Security Bypass Vulnerability
- Microsoft Research JavaScript Cryptography Library Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker
- portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8319
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980935 Nodejs (npm) Security Update for msccrypto (GHSA-qg3g-2mgh-33j8)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)