



CVE-2017-16042

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-16042
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-04 19:29:00 UTC
Updated	2019-10-09 23:24:00 UTC
Description	Growl adds growl notification support to nodejs. Growl before 1.10.2 does not properly sanitize input before passing it to ex

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Growl Project	Growl	All	All	All	All
Application	Growl Project	Growl	All	All	All	All

References

Reference	Source	L
Overview	MISC	n
fix(lib): fixed command injection vulnerability according to Issue #60 by keymandll · Pull Request #61 · tj/node-growl · GitHub	MISC	gi
Unsafe use of exec · Issue #60 · tj/node-growl · GitHub	MISC	gi
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

[984029](#) Nodejs (npm) Security Update for growl (GHSA-qh2h-chj9-jffq)

© [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](#)