



CVE-2017-16137

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

Summary

CVE	CVE-2017-16137
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-07 02:29:00 UTC
Updated	2023-11-07 02:40:00 UTC
Description	The debug module is vulnerable to regular expression denial of service when untrusted user input is passed into the o form

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Pony Mail!	MLIST	lists.apache.org	
Overview	MISC	nodesecurity.io	Third Party Advis
fix: remove ReDoS regexp by zhuangya · Pull Request #504 · visionmedia/debug · GitHub	MISC	github.com	Patch, Third Part
Vulnerable Regular Expression · Issue #501 · visionmedia/debug · GitHub	MISC	github.com	Third Party Advis
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983967 Nodejs (npm) Security Update for debug (GHSA-gxpj-cx7g-858c)

© [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](#)