



CVE-2018-3737

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

Summary

CVE	CVE-2018-3737
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-07 02:29:00 UTC
Updated	2023-01-30 16:06:00 UTC
Description	sshpk is vulnerable to ReDoS when parsing crafted invalid public keys.

Risk And Classification

Problem Types: CWE-185

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joyent	Sshpk	1.13.1	All	All	All
Application	Joyent	Sshpk	1.13.1	All	All	All
Application	Joyent	Sshpk	All	All	All	All

References

Reference	Source	Link	Tags
HackerOne	MISC	hackerone.com	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983409 Nodejs (npm) Security Update for sshpk (GHSA-2m39-62fm-q8r3)

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](#)