



CVE-2018-0492

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

Summary

CVE	CVE-2018-0492
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-03 07:29:00 UTC
Updated	2019-03-14 18:43:00 UTC
Description	Johnathan Nightingale beep through 1.3.4, if setuid, has a race condition that allows local privilege escalation.

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Beep Project	Beep	All	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DSA 4163-1] beep security update	CONFIRM	lists.debian.org	Mailing List, Third
Debian -- Security Information -- DSA-4163-1 beep	DEBIAN	www.debian.org	Third Party Advise
CVE-2018-0492	CONFIRM	security-tracker.debian.org	Third Party Advise
GNU Beep 1.3 - 'HoleyBeep' Local Privilege Escalation - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Third Part
[SECURITY] [DLA 1338-1] beep security update	MLIST	lists.debian.org	Mailing List, Third
beep: Local privilege escalation (GLSA 201805-15) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advise
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical analysis

NVD vulnerability detail

NVD

[nvd.nist.gov](#)

Canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710273 Gentoo Linux beep Local privilege escalation Vulnerability (GLSA 201805-15)

© [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](#)