



CVE-2017-5226

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

Summary

CVE	CVE-2017-5226
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-29 20:59:00 UTC
Updated	2023-03-17 12:15:00 UTC
Description	When executing a program via the bubblewrap sandbox, the nonpriv session can escape to the parent session by using the

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Projectatomic	Bubblewrap	All	All	All	All

References

Reference
oss-security - WebKitGTK and WPE WebKit Security Advisory WSA-2020-0006
Call setsid() before executing sandboxed code (CVE-2017-5226) · projectatomic/bubblewrap@d7fc532 · GitHub
Bubblewrap CVE-2017-5226 Security Bypass Vulnerability
1411811 – (CVE-2017-5226) CVE-2017-5226 bubblewrap: Nonprivileged session can escape to the parent session by using the TIOCSTI ioctl
oss-security - TTY pushback vulnerabilities / TIOCSTI
CVE-2017-5226 -- bubblewrap escape via TIOCSTI ioctl · Issue #142 · projectatomic/bubblewrap · GitHub
oss-security - flatpak: CVE-2023-28100: TIOCLINUX can send commands outside sandbox if running on a virtual console
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)