



# CVE-2017-2616

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-2616
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-27 19:29:00 UTC
<b>Updated</b>	2019-10-09 23:26:00 UTC
<b>Description</b>	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local aut

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Util-linux Project</a>	<a href="#">Util-linux</a>	All	All	All	All
Application	<a href="#">Util-linux Project</a>	<a href="#">Util-linux</a>	All	All	All	All

## References

Reference	Source	Link
<a href="#">su: properly clear child PID · karelzak/util-linux@dffab15 · GitHub</a>	CONFIRM	<a href="#">gith</a>
<a href="#">Red Hat Customer Portal</a>	REDHAT	<a href="#">acc</a>
<a href="#">util-linux CVE-2017-2616 Local Denial of Service Vulnerability</a>	BID	<a href="#">ww</a>
<a href="#">Red Hat Customer Portal</a>	REDHAT	<a href="#">rhn</a>
<a href="#">Shadow: Multiple vulnerabilities (GLSA 201706-02) — Gentoo Security</a>	GENTOO	<a href="#">sec</a>
<a href="#">Util-linux Child Process Race Condition Lets Local Users Kill Root-Owned Processes in Certain Cases - SecurityTracker</a>	SECTRACK	<a href="#">ww</a>
<a href="#">Debian -- Security Information -- DSA-3793-1 shadow</a>	DEBIAN	<a href="#">ww</a>
<a href="#">1418710 – (CVE-2017-2616) CVE-2017-2616 util-linux: Sending SIGKILL to other processes with root privileges via su</a>	CONFIRM	<a href="#">bug</a>
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">ww</a>
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[378252](#) Virtuozzo Linux Security Update for libuuid-devel (VZLSA-2017:0907)

[501249](#) Alpine Linux Security Update for shadow

[710457](#) Gentoo Linux Shadow Multiple Vulnerabilities (GLSA 201706-02)

© 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](https://status.cve.report)**