



# CVE-2020-12826

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

## Summary

<b>CVE</b>	CVE-2020-12826
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-12 19:15:00 UTC
<b>Updated</b>	2021-07-15 19:16:00 UTC
<b>Description</b>	A signal access-control issue was discovered in the Linux kernel before 5.6.5, aka CID-7395ea4e65c2. Because exec_id in

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Mrg</a>	2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Mrg</a>	2.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Mrg</a>	2.0	All	All	All

## References

Reference	Source
kernel-hardening - Curiosity around 'exec_id' and some problems associated with it	MISC
May 2020 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIR
USN-4391-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU
signal: Extend exec_id to 64bits · torvalds/linux@7395ea4 · GitHub	MISC
[SECURITY] [DLA 2241-2] linux security update	MLIST
USN-4369-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.6.5	MISC
1822077 – (CVE-2020-12826) CVE-2020-12826 kernel: possible to send arbitrary signals to a privileged (suidroot) parent process	CONFIR
linux-kernel - Curiosity around 'exec_id' and some problems associated with it	MISC
USN-4367-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU
[SECURITY] [DLA 2241-1] linux security update	MLIST
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)
- [352300](#) Amazon Linux Security Advisory for kernel: ALAC2012-2020-020
- [610324](#) Google Android March 2021 Security Patch Missing for Huawei EMUI
- [900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903235](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3477)
- [906179](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3477-1)
- [940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

© 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](#)**