



# CVE-2022-42896

Published on: Not Yet Published

Last Modified on: 11/28/2022 01:27:00 AM UTC

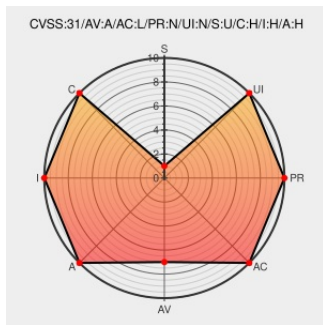
## CVE-2022-42896

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

There are use-after-free vulnerabilities in the Linux kernel's net/bluetooth/l2cap\_core.c's l2cap\_connect and l2cap\_le\_connect\_req functions which may allow code execution and leaking kernel memory (respectively) remotely via Bluetooth. A remote attacker could execute code leaking kernel memory via Bluetooth if within proximity of the

victim. We recommend upgrading past commit <https://www.google.com/url>

<https://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4>

<https://www.google.com/url>

CVE-2022-42896 has been assigned by [G](#) security@google.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [G](#) **Linux - Linux Kernel** version = **3.0.0**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>ADJACENT_NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

## CVE References

Description	Tags	Link
?????????	<a href="#">kernel.dance</a> <a href="#">text/html</a>	<a href="#">MISC kernel.dance/#711f8c3fb3db61897080468586b970c87c61d9e4</a>
Bluetooth: L2CAP: Fix accepting connection request for invalid SPSM · torvalds/linux@711f8c3 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	<a href="#">MISC github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4</a>

By selecting these links, you may be leaving CVEreport webpage. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).



There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

#### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-42896 : There are use-after-free vulnerabilities in the #Linux #kernel's net/bluetooth/l2cap_core.c's l2ca... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-11-23 15:05:42
 /r/netcve	<a href="#">CVE-2022-42896</a>	2022-11-23 15:38:30

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)