

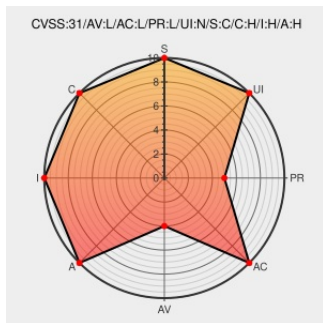


CVE-2020-28921

Published on: 11/27/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-28921

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Pc Analyser](#) from [Pcanalyser](#) contain the following vulnerability:

An issue was discovered in Devid Espenschied PC Analyser through 4.10. The PCADRVX64.SYS kernel driver exposes IOCTL functionality that allows low-privilege users to read and write to arbitrary Model Specific Registers (MSRs). This could lead to arbitrary Ring-0 code execution and escalation of privileges.

CVE-2020-28921 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
GitHub - eset/vulnerability-disclosures: Repository of vulnerabilities disclosed by ESET	Third Party Advisory github.com text/html	MISC github.com/eset/vulnerability-disclosures

Historie – PC Analyser

Release Notes

Vendor Advisory

www.pcanalyser.de

text/html

MISC

www.pcanalyser.de/index.php/historie/

vulnerability-disclosures/CVE-2020-28921.md at master · eset/vulnerability-disclosures · GitHub

Exploit

Third Party Advisory

github.com

text/html

MISC

github.com/eset/vulnerability-disclosures/blob/master/CVE-2020-28921/CVE-2020-28921.md

By selecting these links, you may be leaving CVEreport webspace. 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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pcanalyser	Pc Analyser	All	All	All	All

cpe:2.3:a:pcanalyser:pc_analyser:*****::

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →