CVE-2022-33172

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-33172
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-24 12:15:00 UTC
Updated	2022-08-29 15:48:00 UTC
Description	de.fac2 1.34 allows bypassing the User Presence protection mechanism when there is malware on the victim's PC.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bund	De.fac2	1.34	All	All	All

References

Reference	Source	Link	Tags
Update README.md · BSI-Bund/de.fac2@d3c93c6 · GitHub	MISC	github.com	
GitHub - BSI-Bund/de.fac2: A Common Criteria (CC) and FIDO certified FIDO U2F javacard applet.	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**