



CVE-2020-9331

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

Summary

CVE	CVE-2020-9331
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-23 05:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	CryptoPro CSP through 5.0.0.10004 on 32-bit platforms allows Local Privilege Escalation (by local users with the SeChange

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cryptopro	Csp	All	All	All	All
Application	Cryptopro	Csp	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2020-9361/CVE-2020-9331 CryproPro Privilege Escalation Proof Of Concept - YouTube	MISC	www.youtube.com	Exploit, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, i

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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