CVE-2022-0732

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

Summary

CVE	CVE-2022-0732
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-24 16:15:00 UTC
Updated	2023-06-27 18:11:00 UTC
Description	The backend infrastructure shared by multiple mobile device monitoring services does not adequately authenticate or autho

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	1byte	Copy9	-	All	All	All
Application	1byte	Exactspy	-	All	All	All
Application	1byte	Fonetracker	-	All	All	All
Application	1byte	Guestspy	-	All	All	All
Application	1byte	Ispyoo	-	All	All	All
Application	1byte	Mxspy	-	All	All	All
Application	1byte	Secondclone	-	All	All	All
Application	1byte	Thespyapp	-	All	All	All
Application	1byte	The Truth Spy	-	All	All	All

References

Reference	Source	Link	Tag
CWE - CWE-284: Improper Access Control (4.3)	MISC	cwe.mitre.org	
VU#229438 - Mobile device monitoring services do not authenticate API requests	CERT-VN	kb.cert.org	
VU#229438 - Mobile device monitoring services do not authenticate API requests	CERT-VN	www.kb.cert.org	
Behind the stalkerware network spilling the private phone data of hundreds of thousands – TechCrunch	CONFIRM	techcrunch.com	
CVE Program record	CVE.ORG	www.cve.org	can

NVD vulnerability detail	NVD	nvd.nist.gov	can

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**