CVE-2020-12122

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

Summary

CVE	CVE-2020-12122
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-05 20:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	In Max Secure Max Spyware Detector 1.0.0.044, the driver file (MaxProc64.sys) allows local users to cause a denial of serv

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Maxpcsecure	Max Spyware Detector	1.0.0.044	All	All	All
Application	Maxpcsecure	Max Spyware Detector	1.0.0.044	All	All	All

References

Reference	Source	Link	Tags
Kernel-exploits/MaxProc64.sys at master · FULLSHADE/Kernel-exploits · GitHub	MISC	github.com	Exploit,
Max Secure Spyware Detector:Detect and safely remove spyware and adware from your PC	MISC	www.maxpcsecure.com	Produc
GitHub - FULLSHADE/Kernel-exploits: Windows kernel driver exploits	MISC	github.com	Produc
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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