CVE-2020-36603

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

Summary

CVE	CVE-2020-36603
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-14 22:15:00 UTC
Updated	2022-09-20 16:59:00 UTC
Description	The HoYoVerse (formerly miHoYo) Genshin Impact mhyprot2.sys 1.0.0.0 anti-cheat driver does not adequately restrict unp

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hoyoverse	Mhyprot2	1.0.0.0	All	All	All

References

Reference
Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus
GitHub - kkent030315/evil-mhyprot-cli: A PoC for Mhyprot2.sys vulnerable driver that allowing read/write memory in kernel/user via unprivilege
Disclosure: The Mhyprot Vulnerability - Genshin Impact | GodEye.club
Hackers Are Using Anti-Cheat in 'Genshin Impact' to Ransom Victims
GitHub - kagurazakasanae/Mhyprot2DrvControl: A lib that allows using mhyprot2 driver for enum process modules, r/w process memory and k
CVE Program record
NVD vulnerability detail

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