CVE-2020-6018

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

Summary

CVE	CVE-2020-6018
State	PUBLIC
Assigner	cve@checkpoint.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-02 01:15:00 UTC
Updated	2022-04-12 16:19:00 UTC
Description	Valve's Game Networking Sockets prior to version v1.2.0 improperly handles long encrypted messages in function AES_G(

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Valvesoftware	Game Networking Sockets	All	All	All	All
Application	Valvesoftware	Game Networking Sockets	All	All	All	All

References

Reference	Source	Link	T
Check if output buffer is too small. · ValveSoftware/GameNetworkingSockets@bea84e2 · GitHub	MISC	github.com	P
Game On - Finding vulnerabilities in Valve's "Steam Sockets" - Check Point Research	MISC	research.checkpoint.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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