CVE-2020-6147

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

Summary

CVE	CVE-2020-6147
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-13 15:15:00 UTC
Updated	2022-05-13 20:57:00 UTC
Description	A heap overflow vulnerability exists in Pixar OpenUSD 20.05 when the software parses compressed sections in binary USD

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Application	Pixar	Openusd	20.05	All	All	All
Application	Pixar	Openusd	20.05	All	All	All

References

Reference	Source	Link
TALOS-2020-1094 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosi
Full Disclosure: APPLE-SA-2020-11-13-3 Additional information for APPLE-SA-2020-09-16-1 iOS 14.0 and iPadOS 14.0	FULLDISC	seclis
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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