CVE-2022-22728

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

Summary

CVE	CVE-2022-22728
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-25 15:15:00 UTC
Updated	2023-11-07 03:43:00 UTC
Description	A flaw in Apache libapreq2 versions 2.16 and earlier could cause a buffer overflow while processing multipart form uploads.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Libapreq2	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All

References

Reference	Source	Link	Tag
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
libapreq2: Buffer Overflow (GLSA 202305-20) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 36 Update: libapreq2-2.17-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
[SECURITY] Fedora 37 Update: libapreq2-2.17-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	

oss-security - CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
[SECURITY] Fedora 35 Update: libapreq2-2.17-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 3269-1] libapreq2 security update	MLIST	lists.debian.org	
[SECURITY] Fedora 36 Update: libapreq2-2.17-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
[SECURITY] Fedora 37 Update: libapreq2-2.17-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
lists.apache.org/thread/2fsjoor96d47vtkpf76x4yo06nccvy1y	MISC	lists.apache.org	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.com	
[SECURITY] Fedora 35 Update: libapreq2-2.17-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	www.openwall.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.

Legacy QID Mappings

- 181476 Debian Security Update for libapreq2 (DLA 3269-1)
- 183075 Debian Security Update for libapreq2 (CVE-2022-22728)
- 283109 Fedora Security Update for libapreq2 (FEDORA-2022-cf658a432f)
- 283110 Fedora Security Update for libapreq2 (FEDORA-2022-61f5b492b7)
- 354073 Amazon Linux Security Advisory for libapreq2 : ALAS-2022-1637
- 710721 Gentoo Linux libapreq2 Buffer Overflow Vulnerability (GLSA 202305-20)