



# CVE-2022-22728

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-22728
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-25 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:43:00 UTC
<b>Description</b>	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	<a href="#">Apache</a>	<a href="#">Libapreq2</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All

## References

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

oss-security - CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 35 Update: libapreq2-2.17-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 3269-1] libapreq2 security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 36 Update: libapreq2-2.17-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 37 Update: libapreq2-2.17-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
<a href="http://lists.apache.org/thread/2fsjoor96d47vtkpf76x4yo06nccvy1y">lists.apache.org/thread/2fsjoor96d47vtkpf76x4yo06nccvy1y</a>	MISC	<a href="http://lists.apache.org">lists.apache.org</a>	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 35 Update: libapreq2-2.17-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
oss-security - Re: CVE-2022-22728: libapreq2: libapreq2 multipart form parse memory corruption	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)