



# CVE-2021-38714

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

## Summary

<b>CVE</b>	CVE-2021-38714
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-24 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:37:00 UTC
<b>Description</b>	In Plib through 1.85, there is an integer overflow vulnerability that could result in arbitrary code execution. The vulnerability i

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Fedoraproject</a>	<a href="#">Extra Packages For Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	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
Application	<a href="#">Plib Project</a>	<a href="#">Plib</a>	All	All	All	All
Application	<a href="#">Plib Project</a>	<a href="#">Plib</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 36 Update: plib-1.8.5-30.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: plib-1.8.5-30.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 2775-1] plib security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 35 Update: plib-1.8.5-30.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: plib-1.8.5-30.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: plib-1.8.5-30.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	

PLIB / Bugs / #55 integer overflow for maliciously crafted tga file	MISC	<a href="https://sourceforge.net">sourceforge.net</a>	
[SECURITY] Fedora 35 Update: plib-1.8.5-30.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [178816](#) Debian Security Update for plib (DLA 2775-1)
- [180502](#) Debian Security Update for plib (CVE-2021-38714)
- [282756](#) Fedora Security Update for plib (FEDORA-2022-08022e9452)
- [282757](#) Fedora Security Update for plib (FEDORA-2022-1cf3c9578f)
- [282758](#) Fedora Security Update for plib (FEDORA-2022-bcc0df5180)

© [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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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