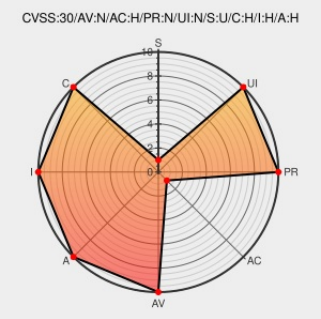
CVE-2021-21772

Published on: 03/10/2021 12:00:00 AM UTC

Last Modified on: 11/16/2022 03:35:00 AM UTC

CVE-2021-21772

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Lib3mf from 3mf contain the following vulnerability:

A use-after-free vulnerability exists in the NMR::COpcPackageReader::releaseZIP() functionality of 3MF Consortium lib3mf 2.0.0. A specially crafted 3MF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.

CVE-2021-21772 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4887-1 lib3mf	www.debian.org Depreciated Link text/html	DEBIAN DSA-4887
[SECURITY] Fedora 34 Update: lib3mf-2.0.1-1.fc34 -	lists.fedoraproject.org	FEDORA FEDORA-2021-bb1b7591c4

package-announce - Fedora Mailing-Lists	text/html	
TALOS-2021-1226 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2021-1226
TALOS-2020-1226 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1226
[SECURITY] Fedora 33 Update: lib3mf-2.0.1-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-b73f9c96ee
3MF Consortium lib3mf: Remote code execution (GLSA 202208-01) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202208-01
[SECURITY] Fedora 32 Update: lib3mf-2.0.1-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-6945629745

Related QID Numbers

178529 Debian Security Update for lib3mf (DSA 4887-1)

180520 Debian Security Update for lib3mf (CVE-2021-21772)

199462 Ubuntu Security Notification for lib3mf Vulnerability (USN-6216-1)

281462 Fedora Security Update for lib3mf (FEDORA-2021-b73f9c96ee)

281463 Fedora Security Update for lib3mf (FEDORA-2021-bb1b7591c4)

281464 Fedora Security Update for lib3mf (FEDORA-2021-6945629745)

710577 Gentoo Linux 3MF Consortium lib3mf Remote code execution Vulnerability (GLSA 202208-01)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	3mf	Lib3mf	2.0.0	-	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating	Fedoraproject	Fedora	34	All	All	All

Operating System	Fedoraproject	Fedora	34	All	All	All

cpe:2.3:a:3mf:lib3mf:2.0.0:-:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | A use-after-free vulnerability exists in... | CVE-2021-21772 | Link for more: alerts.remotelyrmm.com/CVE-2021-21772	2022-05-27 20:32:30
@LinInfoSec	Debian - CVE-2021-21772: talosintelligence.com/vulnerability_…	2022-05-27 21:03:10

← Previous ID

Next ID→