CVE-2021-22204

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-22204
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 18:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	Improper neutralization of user data in the DjVu file format in ExifTool versions 7.44 and up allows arbitrary code execution

Risk And Classification

EPSS: 0.928560000 probability, percentile 0.997650000 (date 2026-04-01)

CISA KEV: Listed on 2021-11-17; due 2021-12-01; ransomware use Unknown

Problem Types: CWE-94

CISA Known Exploited Vulnerability

Vendor	Perl
Product	Exiftool
Name	ExifTool Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-22204

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Exiftool Project	Exiftool	All	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All

References

Reference	Source	L
GitLab Unauthenticated Remote ExifTool Command Injection ≈ Packet Storm	MISC	p
[SECURITY] Fedora 33 Update: perl-Image-ExifTool-12.16-3.fc33 - package-announce - Fedora Mailing-Lists		li
oss-security - Re: [CVE-2021-22204] ExifTool - Arbitrary code execution in the DjVu module when parsing a malicious image	MLIST	w
2021/CVE-2021-22204.json · master · GitLab.org / cves · GitLab	CONFIRM	g
[SECURITY] Fedora 34 Update: perl-Image-ExifTool-12.16-3.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	li
oss-security - [CVE-2021-22204] ExifTool - Arbitrary code execution in the DjVu module when parsing a malicious image	MLIST	w
Debian -- Security Information -- DSA-4910-1 libimage-exiftool-perl	DEBIAN	w
GitLab 13.10.2 Remote Code Execution ≈ Packet Storm	MISC	p
ExifTool DjVu ANT Perl Injection ≈ Packet Storm	MISC	p
[SECURITY] Fedora 32 Update: perl-Image-ExifTool-12.16-3.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	li
[SECURITY] [DLA 2663-1] libimage-exiftool-perl security update	MLIST	li
[SECURITY] Fedora 34 Update: perl-Image-ExifTool-12.16-3.fc34 - package-announce - Fedora Mailing-Lists		li
Update to 12.24 · exiftool/exiftool@cf0f4e7 · GitHub	MISC	g
[SECURITY] Fedora 32 Update: perl-Image-ExifTool-12.16-3.fc32 - package-announce - Fedora Mailing-Lists		li
[SECURITY] Fedora 33 Update: perl-Image-ExifTool-12.16-3.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	li
ExifTool 12.23 Arbitrary Code Execution ≈ Packet Storm	MISC	p
HackerOne	MISC	h
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n
CISA Known Exploited Vulnerabilities catalog	CISA	w

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks vakzz for reporting this vulnerability through the GitLab HackerOne bug bounty program who then reported it to the ExifTool maintainer

Legacy QID Mappings

- 178574 Debian Security Update for libimage-exiftool-perl (DSA 4910-1)
- 178599 Debian Security Update for libimage-exiftool-perl (DLA 2663-1)
- 180151 Debian Security Update for libimage-exiftool-perl (CVE-2021-22204)
- 198405 Ubuntu Security Notification for ExifTool vulnerability (USN-4987-1)
- 281250 Fedora Security Update for perl (FEDORA-2021-de850ed71e)
- 281251 Fedora Security Update for perl (FEDORA-2021-e3d8833d36)

281252 Fedora Security Update for perl (FEDORA-2021-88d24aa32b)

501658 Alpine Linux Security Update for perl-image-exiftool

690820 Free Berkeley Software Distribution (FreeBSD) Security Update for security vulnerability found in exiftool (955f377e-7bc3-11ec-a51c-7533f219d428)

750219 OpenSUSE Security Update for perl-Image-ExifTool (openSUSE-SU-2021:0707-1)