CVE-2021-45463

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

Summary

CVE	CVE-2021-45463
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-23 06:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	load_cache in GEGL before 0.4.34 allows shell expansion when a pathname in a constructed command line is not escaped

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Gegl	Gegl	All	All	All	All
Application	Gimp	Gimp	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
docs/NEWS.adoc · master · GNOME / gegl · GitLab	MISC	gitlab.gn
plug-ins: in file-gegl, use the accurate load/save GEGL operation… (e8a31ba4) · Commits · GNOME / GIMP · GitLab	MISC	gitlab.gn
[SECURITY] Fedora 34 Update: gegl04-0.4.34-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedo
[SECURITY] Fedora 35 Update: gegl04-0.4.34-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedo
[SECURITY] Fedora 34 Update: gegl04-0.4.34-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedo
GIMP 2.10.30 Released - GIMP	MISC	www.gim
[SECURITY] Fedora 35 Update: gegl04-0.4.34-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedo
# Arbitrary Command Execution in load_cache() (#298) · Issues · GNOME / gegl · GitLab	CONFIRM	gitlab.gn

magick-load: use more robust g_spawn_async() instead of system() (bfce470f) · Commits · GNOME / gegl · GitLab	MISC	gitlab.gn
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159596 Oracle Enterprise Linux Security Update for gegl (ELSA-2022-0162)
- 159597 Oracle Enterprise Linux Security Update for gegl04 (ELSA-2022-0177)
- 184786 Debian Security Update for gegl (CVE-2021-45463)
- 240008 Red Hat Update for gegl (RHSA-2022:0162)
- 240009 Red Hat Update for gegl04 (RHSA-2022:0178)
- 240011 Red Hat Update for gegl04 (RHSA-2022:0184)
- 240019 Red Hat Update for gegl04 (RHSA-2022:0177)
- 257145 CentOS Security Update for gegl (CESA-2022:0162)
- 282221 Fedora Security Update for gegl04 (FEDORA-2022-a1c5b18362)
- 282230 Fedora Security Update for gegl04 (FEDORA-2022-5b5a738d7a)
- 353181 Amazon Linux Security Advisory for gegl : ALAS2-2022-1755
- 377019 Alibaba Cloud Linux Security Update for gegl (ALINUX2-SA-2022:0005)
- 502087 Alpine Linux Security Update for gegl
- 671429 EulerOS Security Update for gegl04 (EulerOS-SA-2022-1344)
- 671440 EulerOS Security Update for gegl (EulerOS-SA-2022-1321)
- 671725 EulerOS Security Update for gegl (EulerOS-SA-2022-1722)
- 751562 SUSE Enterprise Linux Security Update for gegl (SUSE-SU-2021:4193-1)
- 751574 OpenSUSE Security Update for gegl (openSUSE-SU-2021:4209-1)
- 751575 OpenSUSE Security Update for gegl (openSUSE-SU-2021:4210-1)
- 940432 AlmaLinux Security Update for gegl04 (ALSA-2022:0177)
- 960836 Rocky Linux Security Update for gegl04 (RLSA-2022:0177)