CVE-2020-12658

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

Summary

CVE	CVE-2020-12658
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-31 01:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	** DISPUTED ** gssproxy (aka gss-proxy) before 0.8.3 does not unlock cond_mutex before pthread exit in gp_worker_mair

Risk And Classification

Problem Types: CWE-667

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gssproxy Project	Gssproxy	All	All	All	All
Application	Gssproxy Project	Gssproxy	All	All	All	All

References

Reference	Source	Link	Tags
Comparing v0.8.2...v0.8.3 · gssapi/gssproxy · GitHub	MISC	github.com	Third Par
Unlock cond_mutex before pthread exit in gp_worker_main() · gssapi/gssproxy@cb76141 · GitHub	MISC	github.com	Patch, Th
[SECURITY] [DLA 2516-1] gssproxy security update	MLIST	lists.debian.org	Mailing Li
Commit - gssproxy - cb761412e299ef907f22cd7c4146d50c8a792003 - Pagure.io	MISC	pagure.io	Third Par
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

174872 SUSE Enterprise Linux Security Update for gssproxy (SUSE-SU-2021:1030-1)

174873 SUSE Enterprise Linux Security Update for gssproxy (SUSE-SU-2021:1029-1)

670179 EulerOS Security Update for gssproxy (EulerOS-SA-2021-1679)

670281 EulerOS Security Update for gssproxy (EulerOS-SA-2021-1795)

670918 EulerOS Security Update for gssproxy (EulerOS-SA-2021-1145)

750277 OpenSUSE Security Update for gssproxy (openSUSE-SU-2021:0531-1)