CVE-2020-13614

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

Summary

CVE	CVE-2020-13614
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-26 23:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	An issue was discovered in ssl.c in Axel before 2.17.8. The TLS implementation lacks hostname verification.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axel Project	Axel	All	All	All	All
Application	Axel Project	Axel	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference
Axel may not verify server certificate CN/SAN/hostname (allowing SSL interception) · Issue #262 · axel-download-accelerator/axel · GitHub
[SECURITY] Fedora 34 Update: axel-2.17.10-1.fc34 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 33 Update: axel-2.17.10-1.fc33 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 34 Update: axel-2.17.10-1.fc34 - package-announce - Fedora Mailing-Lists
Release Version 2.17.8 · axel-download-accelerator/axel · GitHub
[SECURITY] Fedora 33 Update: axel-2.17.10-1.fc33 - package-announce - Fedora Mailing-Lists
[security-announce] openSUSE-SU-2020:0785-1: moderate: Security update f
[security-announce] openSUSE-SU-2020:0778-1: moderate: Security update f
CVE Program record

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

281248 Fedora Security Update for axel (FEDORA-2021-5214bd8f14)

281249 Fedora Security Update for axel (FEDORA-2021-90b4716992)

500045 Alpine Linux Security Update for axel

503727 Alpine Linux Security Update for axel

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**