



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	1
[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	1
[SECURITY] Fedora 34 Update: axel-2.17.10-1.fc34 - package-announce - Fedora Mailing-Lists	1
Release Version 2.17.8 · axel-download-accelerator/axel · GitHub	1
[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	5
[security-announce] openSUSE-SU-2020:0778-1: moderate: Security update f	5
CVE Program record	1

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)