CVE-2020-15173

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

Summary

CVE	CVE-2020-15173
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 23:15:00 UTC
Updated	2021-11-18 17:48:00 UTC
Description	In ACCEL-PPP (an implementation of PPTP/PPPoE/L2TP/SSTP), there is a buffer overflow when receiving an l2tp control

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Accel-ppp	Accel-ppp	All	All	All	All

References

Reference
A possible heap buffer overflow when receiving an l2tp control packet with an AVP which type is a string and no hidden flags, length set to les
l2tp: fix RCE through buffer overflow & fix LE/BE compatibility · accel-ppp/accel-ppp@2324bcd · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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