



CVE-2022-24705

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-24705
State	PUBLIC
Assigner	cve_disclosure@tech.gov.sg
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-14 22:15:00 UTC
Updated	2022-02-19 04:16:00 UTC
Description	The rad_packet_rcv function in radius/packet.c suffers from a memcpy buffer overflow, resulting in an overly-large rcvfrom

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	Source	Link
fix buffer overflow when receive radius packet by svlobanov · Pull Request #35 · accel-ppp/accel-ppp · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Chloe Ong from Government Technology Agency of Singapore

LEGACY: Eugene Lim from Government Technology Agency of Singapore

LEGACY: Kar Wei Loh from Government Technology Agency of Singapore

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

© [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](#)