



Ericsson Packet Core Controller (PCC) - Improper Handling of Syntactically Invalid Structure Vulnerability

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

Summary

CVE	CVE-2024-53828
State	PUBLISHED
Assigner	ERIC
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 10:16:14 UTC
Updated	2026-04-01 14:23:37 UTC
Description	Ericsson Packet Core Controller (PCC) versions prior to 1.38 contain a vulnerability where an attacker sending a large volume of syntactically invalid structures can cause a denial of service.

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from 85b1779b-6ecd-4f52-bcc5-73eac4659dcf

CVSS: 3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.000160000 probability, percentile 0.033390000 (date 2026-04-01)

Problem Types: CWE-228 | CWE-228 CWE-228

Version	Source	Type	Score	Severity	Vector
3.1	85b1779b-6ecd-4f52-bcc5-73eac4659dcf	Secondary	5.3	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ericsson	Packet Core Controller PCC	affected 1.38 1.38	Not specified

References

Reference	Source	Link	Tags
www.ericsson.com/en/about-us/security/psirt/CVE-2024-53828	85b1779b-6ecd-4f52-bcc5-73eac4659dcf	www.ericsson.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: [The UK's National Cyber Security Centre \(NCSC\) \(en\)](#)

CNA: [The UK Telecoms Lab \(UKTL\) \(en\)](#)

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](#).

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