

# Security Bulletin – Ericsson Packet Core Controller (PCC), April 2026

## Summary:

Ericsson has released an update for Packet Core Controller to address a security issue that if exploited may cause service degradation.

## Vulnerability description:

**CVE-2024-53828** - Ericsson Packet Core Controller (PCC) versions prior to 1.38 contain a vulnerability where an attacker sending a large volume of specially crafted messages may cause service degradation.

**CVSS Base Score:** 5.3

**Severity:** Medium

**CVSS Vector:** [CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)

**Weakness Type:** CWE-228: Improper Handling of Syntactically Invalid Structure

## Security update:

The following table lists the Ericsson products affected, versions affected, and the updated version that includes this security update.

To protect your system, download and install the updated version.

CVE Addressed	Product Name	Affected Versions	Updated Versions
CVE-2024-53828	Packet Core Controller (PCC)	All versions prior to PCC 1.38	PCC 1.38

## Acknowledgement:

Ericsson thanks following people/organization for reporting this issue to us:

- The UK's National Cyber Security Centre (NCSC)
- The UK Telecoms Lab (UKTL)



## Additional information:

- Ericsson severity assessment of a vulnerability is based on an average of risk across a diverse set of installed systems and may not represent the true risk to your organization. We recommend evaluating the risk to your specific configuration.
- If you have any questions regarding this bulletin, please reach out to your local Ericsson support representative, for more information see our [Customer Support page](#).
- Learn more about the vulnerability management process followed by the Ericsson Product Security Incident Response Team (PSIRT), see [Ericsson PSIRT page](#).

## Revision history:

Revision	Date	Description
1.0	April 1, 2026	Initial Release

© Ericsson AB 2026. All rights reserved. No part of this message may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this message. For questions, please contact Ericsson Local Support or connect with us on the Omni Network Channel section of My Ericsson. Visit us at Support User Preferences to unsubscribe.