



UID Regex Bypass

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

Summary

CVE	CVE-2026-29133
State	PUBLISHED
Assigner	NCSC.ch
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-02 09:16:21 UTC
Updated	2026-04-16 19:06:51 UTC
Description	SEPPmail Secure Email Gateway before version 15.0.3 allows an attacker to upload PGP keys with UIDs that do not match

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from vulnerability@ncsc.ch

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000510000 probability, percentile 0.156620000 (date 2026-04-21)

Problem Types: CWE-20 | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
4.0	vulnerability@ncsc.ch	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N
3.1	nvd@nist.gov	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Seppmail	Secure Email Gateway	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SEPPmail	Secure Email Gateway	affected 15.0.3 custom	Not specified

References

Reference	Source	Link	Tags
downloads.seppmail.com/extrelnotes/150/ERN15.0.html	vulnerability@ncsc.ch	downloads.seppmail.com	Release Notes
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: [Andris Suter-Dörig \(en\)](#)

CNA: [Matteo Scarlata \(en\)](#)

CNA: [Kenny Paterson \(en\)](#)

Additional Advisory Data

Source	Time	Event
CNA	2025-10-31T14:22:00.000Z	Vulnerability disclosed to SEPPmail
CNA	2026-03-03T00:00:00.000Z	Version 15.0.3 released

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