



# GINA Domain Switch

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-29134
<b>State</b>	PUBLISHED
<b>Assigner</b>	NCSC.ch
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-02 09:16:21 UTC
<b>Updated</b>	2026-04-16 19:03:15 UTC
<b>Description</b>	SEPPmail Secure Email Gateway before version 15.0.3 allows an external user to modify GINA webdomain metadata and I

## 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:L/VI:L/VA:N/SC:L/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:** 0.000560000 probability, percentile 0.176230000 (date 2026-04-21)

**Problem Types:** CWE-807 | CWE-807 CWE-807 Reliance on Untrusted Inputs in a Security Decision

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:L/VI:L/VA:N/SC:L/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
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

**Low**

User Interaction

**None**

**None**  
 Confidentiality  
**Low**  
 Integrity  
**Low**  
 Availability  
**None**  
 Sub Conf.  
**Low**  
 Sub Integrity  
**Low**  
 Sub Availability  
**None**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/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

CVSS v3.1 Breakdown

Attack Vector  
**Network**  
 Attack Complexity  
**Low**  
 Privileges Required  
**None**  
 User Interaction  
**None**  
 Scope  
**Unchanged**  
 Confidentiality  
**None**  
 Integrity  
**High**  
 Availability  
**None**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/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
<a href="https://downloads.seppmail.com/extrelnotes/150/ERN15.0.html">downloads.seppmail.com/extrelnotes/150/ERN15.0.html</a>	<a href="mailto:vulnerability@ncsc.ch">vulnerability@ncsc.ch</a>	<a href="https://downloads.seppmail.com">downloads.seppmail.com</a>	Release Notes
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)