



# CVE-2022-43974

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

## Summary

<b>CVE</b>	CVE-2022-43974
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-09 09:15:00 UTC
<b>Updated</b>	2023-01-13 13:11:00 UTC
<b>Description</b>	MatrixSSL 4.0.4 through 4.5.1 has an integer overflow in matrixSslDecodeTls13. A remote attacker might be able to send a

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Matrixssl</a>	<a href="#">Matrixssl</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Buffer Overflow in MatrixSSL - Advisory · matrixssl/matrixssl · GitHub	CONFIRM	<a href="#">github.com</a>	
<a href="#">www.telekom.com/en/company/data-privacy-and-security/news/advisories-504842</a>	MISC	<a href="#">www.telekom.com</a>	
matrixssl/CHANGES_v4.x.md at 4-6-0-open · matrixssl/matrixssl · GitHub	CONFIRM	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)**