



CVE-2021-26787

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-26787
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-15 07:15:00 UTC
Updated	2023-11-07 03:31:00 UTC
Description	A cross site scripting (XSS) vulnerability in Genesys Workforce Management 8.5.214.20 can occur (during record deletion)

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Genesys	Workforce Management	8.5.214.20	All	All	All

References

Reference	Source
Contact Center Solutions Omnichannel Customer Experience Genesys	MISC
Cross Site Scripting Vulnerability within Genesys Workforce Management version 8.5.214.20 by Liam B Medium	
Cross Site Scripting Vulnerability within Genesys Workforce Management version 8.5.214.20 by Liam B Oct, 2021 Medium	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)