



CVE-2022-38653

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-38653
State	PUBLIC
Assigner	psirt@hcl.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-19 11:15:00 UTC
Updated	2023-11-07 03:50:00 UTC
Description	In HCL Digital Experience, customized XSS payload can be constructed such that it is served in the application unencoded

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcltech	Digital Experience	8.5	All	All	All
Application	Hcltech	Digital Experience	9.0	All	All	All
Application	Hcltech	Digital Experience	9.5	All	All	All

References

Reference

- Security Bulletin: HCL Digital Experience is susceptible to open redirects (CVE-2022-38662) and XSS (CVE-2022-38653) - Customer Support
- CVE Program record
- NVD vulnerability detail

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report