



# CVE-2022-27546

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

## Summary

<b>CVE</b>	CVE-2022-27546
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@hcl.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-29 16:15:00 UTC
<b>Updated</b>	2022-09-01 20:53:00 UTC
<b>Description</b>	HCL iNotes is susceptible to a Reflected Cross-site Scripting (XSS) vulnerability caused by improper validation of user-suppl

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcltech	Domino	10.0	All	All	All
Application	Hcltech	Domino	10.0.1	-	All	All
Application	Hcltech	Domino	10.0.1	fixpack_1	All	All
Application	Hcltech	Domino	10.0.1	fixpack_2	All	All
Application	Hcltech	Domino	10.0.1	fixpack_3	All	All
Application	Hcltech	Domino	10.0.1	fixpack_4	All	All
Application	Hcltech	Domino	10.0.1	fixpack_5	All	All
Application	Hcltech	Domino	10.0.1	fixpack_6	All	All
Application	Hcltech	Domino	10.0.1	fixpack_7	All	All
Application	Hcltech	Domino	10.0.1	fixpack_8	All	All
Application	Hcltech	Domino	11.0	All	All	All
Application	Hcltech	Domino	11.0.1	-	All	All
Application	Hcltech	Domino	11.0.1	fixpack_1	All	All
Application	Hcltech	Domino	11.0.1	fixpack_2	All	All
Application	Hcltech	Domino	11.0.1	fixpack_3	All	All
Application	Hcltech	Domino	11.0.1	fixpack_4	All	All
Application	Hcltech	Domino	11.0.1	fixpack_5	All	All

Application	Hcltech	Domino	12.0	All	All	All
Application	Hcltech	Domino	12.0.1	-	All	All
Application	Hcltech	Domino	12.0.1	fixpack_1	All	All
Application	Hcltech	Domino	9.0	All	All	All
Application	Hcltech	Domino	9.0.1	-	All	All
Application	Hcltech	Domino	9.0.1	fixpack_10	All	All
Application	Hcltech	Domino	9.0.1	fixpack_3	All	All
Application	Hcltech	Domino	9.0.1	fixpack_4	All	All
Application	Hcltech	Domino	9.0.1	fixpack_5	All	All
Application	Hcltech	Domino	9.0.1	fixpack_6	All	All
Application	Hcltech	Domino	9.0.1	fixpack_7	All	All
Application	Hcltech	Domino	9.0.1	fixpack_8	All	All
Application	Hcltech	Domino	9.0.1	fixpack_9	All	All
Application	Hcltech	Hcl Inotes	10.0	All	All	All
Application	Hcltech	Hcl Inotes	10.0.1	-	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_1	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_2	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_3	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_4	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_5	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_6	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_7	All	All
Application	Hcltech	Hcl Inotes	10.0.1	fixpack_8	All	All
Application	Hcltech	Hcl Inotes	11.0	All	All	All
Application	Hcltech	Hcl Inotes	11.0.1	-	All	All
Application	Hcltech	Hcl Inotes	11.0.1	fixpack_1	All	All
Application	Hcltech	Hcl Inotes	11.0.1	fixpack_2	All	All
Application	Hcltech	Hcl Inotes	11.0.1	fixpack_3	All	All
Application	Hcltech	Hcl Inotes	11.0.1	fixpack_4	All	All
Application	Hcltech	Hcl Inotes	11.0.1	fixpack_5	All	All
Application	Hcltech	Hcl Inotes	12.0	All	All	All
Application	Hcltech	Hcl Inotes	12.0.1	-	All	All
Application	Hcltech	Hcl Inotes	12.0.1	fixpack_1	All	All
Application	Hcltech	Hcl Inotes	9.0.1	-	All	All
Application	Hcltech	Hcl Inotes	9.0.1	fixpack_10	All	All

Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_3	All	All
Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_4	All	All
Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_5	All	All
Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_6	All	All
Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_7	All	All
Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_8	All	All
Application	<a href="#">Hcltech</a>	<a href="#">Hcl Inotes</a>	9.0.1	fixpack_9	All	All

## References

Reference	Status
Security Bulletin: HCL iNotes is susceptible to a Reflected Cross-site Scripting (XSS) vulnerability (CVE-2022-27546) - Customer Support	S
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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](#)