



CVE-2023-28008

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

Summary

CVE	CVE-2023-28008
State	PUBLIC
Assigner	psirt@hcl.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-26 20:15:00 UTC
Updated	2023-05-05 20:28:00 UTC
Description	HCL Workload Automation 9.4, 9.5, and 10.1 are vulnerable to an XML External Entity Injection (XXE) attack when process

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcltech	Workload Automation	10.1.0	-	All	All
Application	Hcltech	Workload Automation	9.4.0	-	All	All
Application	Hcltech	Workload Automation	9.4.0	fix_pack_3	All	All
Application	Hcltech	Workload Automation	9.4.0	fix_pack_4	All	All
Application	Hcltech	Workload Automation	9.4.0	fix_pack_5	All	All
Application	Hcltech	Workload Automation	9.4.0	fix_pack_6	All	All
Application	Hcltech	Workload Automation	9.4.0	fix_pack_7	All	All
Application	Hcltech	Workload Automation	9.5.0	-	All	All
Application	Hcltech	Workload Automation	9.5.0	fix_pack_1	All	All
Application	Hcltech	Workload Automation	9.5.0	fix_pack_2	All	All
Application	Hcltech	Workload Automation	9.5.0	fix_pack_3	All	All
Application	Hcltech	Workload Automation	9.5.0	fix_pack_4	All	All
Application	Hcltech	Workload Automation	9.5.0	fix_pack_5	All	All
Application	Hcltech	Workload Automation	9.5.0	fix_pack_6	All	All

References

Reference	Source	Link
-----------	--------	------

Security Bulletin: HCL Workload Automation is vulnerable to multiple security vulnerabilities - Customer Support	MISC	support.hcltec
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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