



CVE-2021-40348

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

Summary

CVE	CVE-2021-40348
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-01 05:15:00 UTC
Updated	2022-11-14 13:30:00 UTC
Description	Spacewalk 2.10, and derivatives such as Uyuni 2021.08, allows code injection. rhn-config-satellite.pl doesn't sanitize the co

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spacewalk Project	Spacewalk	2.10	All	All	All
Application	Uyuni-project	Uyuni	2021.08	All	All	All
Application	Uyuni Project	Uyuni	2021.08	All	All	All

References

Reference	Source	Link
oss-security - spacewalk-admin: CVE-2021-40348: arbitrary local code execution by 'tomcat' user via rhn-config-satellite.pl	MISC	www
Merge pull request #4414 from uyuni-project/Uyuni-2021.09 · uyuni-project/uyuni@790c738 · GitHub	CONFIRM	gith
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160580 Oracle Enterprise Linux Security Update for spacewalk-admin (ELSA-2023-12331)

© [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](#)